

Contents

I	Abstract	1
II	The $\mathbb{F}_2$-vector space $\mathbb{F}_2^n$	2
III	The G_n group	2
IV	A G_n group action on $\mathbb{F}_2^n$	3
V	The n-cube graph	4
VI	The subgroups of G_n	4
VII	A distance on G_n	12
VIII	A partition of G_n by degrees	14
IX	The isometric group $\mathcal{I}_{\text{som}}$	15
X	The γ-core of G_n	18
XI	The property P_o	18
XII	Some G_n partitions	20
XIII	The case P_o	26
XIV	Existence and unicity theorem	29
XV	The prisoners' conundrum	30
XVI	Solving the puzzle	30
XVII	Game strategy	32
XVIII	Let's play a bit with the chessboard	34
XIX	Epilog	37

The prisoners and the n cube puzzle

- Cypher a number in an n-cube

I Abstract

We first present a few tools to solve “The prisoners and the n-cube/chessboard puzzle” which is described in chapter XV on page 30 , then we calculate solutions where they exist, and eventually solve the puzzle (see “Let’s play a bit with the chessboard” chapter XVII on page 34 for application).

II The $\mathbb{F}_2$ -vector space $\mathbb{F}_2^n$

Back to “Solving the puzzle”: chapter XVI on page 31

Back to Case 4 chapter XIII on page 26

We denote $\mathbb{F}_2$ the field $\mathbb{Z}/(2)$, where (2) is the ideal of the $\mathbb{Z}$ ring generated by 2 ($\mathbb{F}_2 = \{0, 1\}$). For n integer, $\mathbb{F}_2^n$ (We define $\mathbb{F}_2^0 = \{0\}$), is the n times product of $\mathbb{F}_2$ -vector space $\mathbb{F}_2$, by definition isomorphic to $\mathbb{F}_2[X]_{n-1}$ the polynomials of order equal or inferior to $n-1$ (for n strictly positive).

Let's consider the injection: $\mathbb{F}_2 \xrightarrow{\delta} \mathbb{Z}$, $\delta(0) \underset{\text{def.}}{=} 0$, $\delta(1) \underset{\text{def.}}{=} 1$, this yields an injection, δ^* from $\mathbb{F}_2[X]$ to $\mathbb{Z}[X]$:

$$s = \sum_I a_i X^i \in \mathbb{F}_2[X], \quad \delta^*(s) \underset{\text{def.}}{=} \sum_I \delta(a_i) X^i \in \mathbb{Z}[X] \quad I \subset \mathbb{N} \quad I \text{ finite}$$

Now considering:

$$\begin{array}{ccc} \mathbb{F}_2[X] & \longrightarrow & \mathbb{N} \\ s & \longmapsto & \delta^*(s)(2) \end{array}$$

this mapping is bijective¹ and we have the following scheme:

$$\begin{array}{lcl} \text{so :} & \mathbb{F}_2^n & \hookrightarrow \mathbb{N} \\ & s & \sim \delta^*(s)(2) \quad (\text{Count in base 2}) \\ \text{Example:} & \mathbb{F}_2^3 \ni (1, 1, 0) & \sim 1 + 2 = 3 \end{array}$$

Remark: $|\mathbb{F}_2^n| = |\mathbb{F}_2|^n = 2^n$

III The G_n group

Back to Epilog, chapter XIX on page 37

$I_n = [1, n]$, n non zero integer, $e_i = (0, 0, \dots, \underbrace{1}_{i\text{th}}, \dots, 0) \in \mathbb{F}_2^n$ we set $I_0 = \emptyset$

An affine space on $\mathbb{F}_2$ is isomorphic to a $\mathbb{F}_2$ -vector space, we confound the two, and let β_i be the affine symmetry defined by:

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\beta_i} & \mathbb{F}_2^n \\ s & \longmapsto & \beta_i(s) = s + e_i \end{array}$$

Example: $\beta_2(0, 1, 1) = (0, 1, 1) + (0, 1, 0) = (0, 0, 1)$ Back to “Game strategy”: chapter XVII on page 32

Let G_n be the abelian group generated by: $\mathbb{B}_n = \{\beta_1, \beta_2, \dots, \beta_n\}$ we set $\mathbb{B}_0 = \emptyset$

$(G_n, \circ)$ is a free abelian group.²

We will denote: $G_o = \{1\}$, $\beta_o = 1$

1

Thanks to Euclidean division by iteration we can find $s \in \mathbb{F}_2[X]$ such that $\delta^*(s)(2) = n$ for any integer n , and this splitting is unique so that $\delta^*(s)$ is uniquely defined, since δ^* is injective, so is s .

2

We define $\prod_{\emptyset} \beta_i = 1$ (and $\sum e_i = 0$)

- commutativity: $\beta_i \beta_j = \beta_j \beta_i \quad i, j \in I_n$, straightforward,
- associativity: $\beta_i (\beta_j \beta_k) = (\beta_i \beta_j) \beta_k \quad i, j, k \in I_n$, straightforward,
- $1 \in G_n$, identity and for $i \in I_n \quad \beta_i^2 = 1 \Rightarrow \beta^2 = 1$ for any $\beta \in G_n$.

Property: $\beta^2 = 1$ for every $\beta \in G_n$, 1 stands for identity.

[Back to embedding proof in footnote 24 on page 10](#)

We have a handy homomorphism μ from G_n to $\mathbb{F}_2^n$:³ [Back to filling out the board: footnote 75 on page 34](#)

[Back to unicity proof: footnote 3 on page 24](#)

$$\mu: \begin{array}{ccc} G_n & \xrightarrow{\mu} & \mathbb{F}_2^n \\ \prod \beta_i & \mapsto & \mu(\prod \beta_i) \stackrel{\text{def.}}{=} \sum_I e_i \end{array}$$

Clearly μ is surjective, G_n contains at most $\sum_0^n \binom{n}{k} = 2^n$ elements, so $|G_n| = |\mathbb{F}_2^n|$, hence μ is injective, it is an isomorphism: $(G_n, \circ) \stackrel{\mu}{\sim} (\mathbb{F}_2^n, +)$

Property: $\beta \in G_n \quad \exists! I \in \mathcal{P}(I_n), \quad \beta = \prod_I \beta_i \sim \sum_I 2^{i-1}$ ⁴ [Back to unicity, proof in footnote 3 on page 24](#)
[Back to “A distance on \$G_n\$ ”: chapter VII on page 12](#) As a consequence:

$$\mu^*: \begin{array}{ccc} \mathcal{P}(I_n) & \xrightarrow{\mu^*} & G_n \\ J & \mapsto & \prod_J \beta_i \end{array}$$

is an isomorphism.

- It is a homomorphism: $\prod_{I+J} \beta_i = \prod_I \beta_i \prod_J \beta_i, I, J \in \mathcal{P}(I_n)$
- it is surjective, thus bijective

[Back to “Epilog”: chapter XIX on page 37](#)

IV A G_n group action on $\mathbb{F}_2^n$

[Back to “Solving the puzzle”: chapter XVI on page 31](#)

We define an action on $\mathbb{F}_2^n$ like this: $\beta \in G_n, s \in \mathbb{F}_2^n \quad \beta.s \stackrel{\text{def.}}{=} s + \mu(\beta)$ ⁵

³

$I, J, K \subset I_n$, we use addition in $(\mathcal{P}(I_n), +)$ the boolean group

$$\psi(\prod_J \beta_i \prod_K \beta_i) = \psi(\prod_{J+K} \beta_i) = \sum_{J+K} e_i$$

$$\psi(\prod_J \beta_i) + \psi(\prod_K \beta_i) = \sum_J e_i + \sum_K e_i = \sum_{J+K} e_i$$

⁴

Let be $I, I' \in \mathcal{P}(I_n)$ such that $\beta = \prod_I \beta_i = \prod_{I'} \beta_i, 1 = \beta^2 = \prod_{I+I'} \beta_i, I + I' = \emptyset, I = I'$

⁵

This is actually an action:

- $\beta, \gamma \in G_n, s \in \mathbb{F}_2^n \quad (\beta\gamma).s = s + \mu(\beta\gamma) = s + \mu(\beta) + \mu(\gamma) = \beta.(s + \mu(\gamma)) = \beta.(\gamma.s)$
- $1.s = s + \mu(1) = s$

Property: $\beta, \gamma \in G_n \quad \beta \cdot \mu(\gamma) = \mu(\beta) + \mu(\gamma) = \mu(\beta\gamma)$

This action is:

• transitive, there's only one orbit: $\mu(\gamma) \in \mathbb{F}_2^n, G_n \cdot \mu(\gamma) = \mu(G_n \gamma) = \mu(G_n)$ ⁶

• free (The stabilizer of any s in $\mathbb{F}_2^n$ is trivial): $\beta \cdot s = s$ implies $\beta = 1$ for $s \in \mathbb{F}_2^n$ ⁷

And so this action is simply transitive.

[Back to “Epilog”: chapter XIX on page 37](#)

Eventually, the action of G_n upon $\mathbb{F}_2^n$ is isomorphic to group operation in G_n :

$$\beta \in G_n, s \in \mathbb{F}_2^n, \quad \beta \cdot s \stackrel{\mu^{-1}}{\sim} \beta \mu^{-1}(s)$$

V The n-cube graph

We define the n-cube, as the graph whose vertices are $\mathbb{F}_2^n$ and edges:⁸ $A_n = \{(s, \beta \cdot s), s \in \mathbb{F}_2^n, \beta \in \mathbb{B}_n\}$.

Example: 0-cube is: $(\{O\}, \emptyset)$, $O = (0)$ (See figure: 1 on the next page).

(The n-cube graph is an Eulerian graph.) [Back to “Epilog”, chapter XIX on page 37](#)

VI The subgroups of G_n

We consider $(\mathcal{P}(G_n))$ the boolean group. [Back to “Epilog” in chapter XIX on page 37](#)

To simplify the script, for $\{\beta\} \in \mathcal{P}(G_n)$ we write simply β instead (Thus: $\{\beta_1, \beta_2\} = \beta_1 + \beta_2, \quad \beta_1, \beta_2 \in G_n$).

Now we construct the product $\bullet$ in $\mathcal{P}(G_n)$.

$$I, J \subset I_{2^n} \quad A = \sum_I a_i \in \mathcal{P}(G_n), \quad B = \sum_J a_i \in \mathcal{P}(G_n), \quad a_i \in G_n$$

$$A \bullet B \stackrel{\text{def.}}{=} \sum_{I \times J} a_i a_j$$

6

$$g, \gamma \in G_n, g\gamma \in G_n, g\gamma\gamma \in G_n\gamma, g \in G_n\gamma, G_n \subset G_n\gamma, G_n = G_n\gamma$$

7

$$\beta \cdot s = s, s = s + \mu(\beta), 2s = 2s + \mu(\beta), \text{car}(\mathbb{F}_2) = 2, 0 = \mu(\beta), \beta = 1$$

8

Let's consider the affine space $O + \mathbb{F}_2^n$ on field $\mathbb{F}_2$. Since it is isomorphic to $\mathbb{F}_2^n$, we denote it: $\mathbb{F}_2^n$. $O = (0, \dots, 0) \in \mathbb{F}_2^n$.

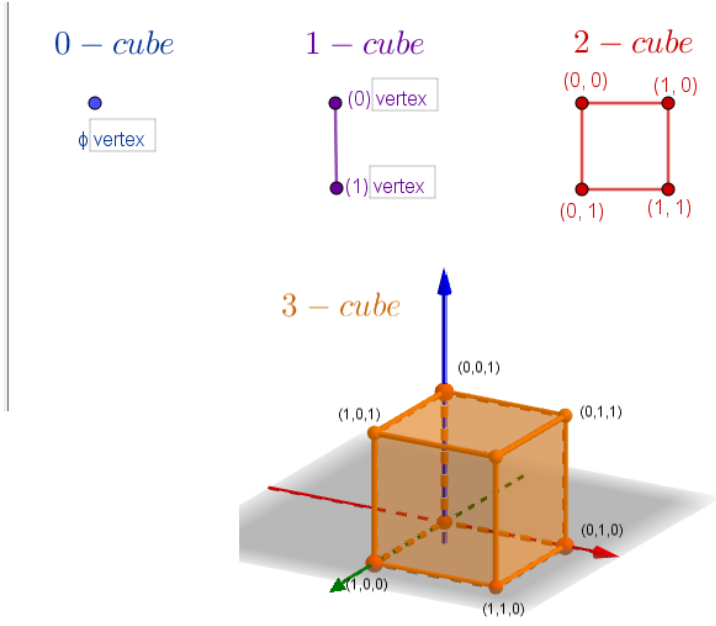
$$\mathbb{F}_2 = \beta_1(O) + \{O\} = (1 + \beta_1) \bullet \{O\} \quad A_1 = \left\{ \left(\{O\}, \beta_1(O) \right) \right\} \text{ For a definition of operation “}\bullet\text{” see VI}$$

$$\begin{aligned} \mathbb{F}_2^2 &= (\beta_2 + 1) \bullet \mathbb{F}_2 \quad A_2 = \left\{ \left(\{O\}, \beta_1(O) \right), \left(\{O\}, \beta_2(O) \right), \left(\beta_1(O), \beta_2\beta_1(O) \right), \left(\beta_2(O), \beta_1\beta_2(O) \right) \right\} \\ \mathbb{F}_2^n &= \prod_{I_n} (1 + \beta_i) \{O\} = G_n \bullet \{O\} \end{aligned}$$

We stretch $\mathbb{F}_2^n$ in the $n + 1$ dimension by means of the translation β_{n+1} and add it up to $\mathbb{F}_2^n \bullet \{O\}$ to obtain $\mathbb{F}_2^{n+1} \bullet \{O\}$.

So the n-cube graph is the affine space $\mathbb{F}_2^n \bullet \{O\}$ as vertices adjoined with the edges generated by the stretches at each step.

Figure 1: The n-cubes



$(\mathcal{P}(G_n), \bullet)$ is a commutative monoid⁹

$(\mathcal{P}(G_n), \bullet, +)$ is a commutative ring¹⁰

Later on we will write AB instead of $A \bullet B$, whereby: $G_n = \prod_{I_n} (1 + \beta_i) = \prod_{\mathbb{B}_n} (1 + \beta)$ ¹¹

9

- commutativity: G_n abelian
- identity: $I \subset I_2^n$, $A = \sum_I a_i \in \mathcal{P}(G_n)$, $A \bullet 1 = \sum_I a_i 1 = \sum_I a_i = A$, $1 \bullet A = A$
- associativity: $I, J, K \subset I_2^n$, $A = \sum_I a_i$, $B = \sum_J a_i$, $C = \sum_K a_i \in \mathcal{P}(G_n)$
 $A \bullet (B \bullet C) = \sum_I a_i \sum_{JxK} a_j a_k = \sum_{IxJxK} a_i a_j a_k = \sum_{IxJ} a_i a_j \sum_K a_k = (A \bullet B) \bullet C$

10

- $(\mathcal{P}(G_n), +)$ is an abelian group (The Boolean group) and,
- distributivity: $I, J, K \subset I_2^n$, $A = \sum_I a_i$, $B = \sum_J a_i$, $C = \sum_K a_i \in \mathcal{P}(G_n)$
 $A \bullet (B + C) = \sum_I a_i \sum_{J+K} a_j = \sum_{Ix(J+K)} a_i a_j$ $A \bullet B + A \bullet C = \sum_{IxJ} a_i a_j + \sum_{IxK} a_i a_k$
 for $j = k$ the sum $a_i a_j + a_i a_k = \emptyset$, $A \bullet B + A \bullet C = \sum_{Ix(J+K)} a_i a_j$

11

Since $\prod_{\mathbb{B}_n} (1 + \beta)$ contains $\sum_0^n \binom{n}{k} = 2^n$ distinct elements.

Automorphism on $G_n, \text{Aut}(G_n)$

Example: $\sigma \in \mathcal{T}(I_n)$ the permutations of $I_n, I \in \mathcal{P}(I_n)$,

$$\varphi_\sigma : \begin{array}{ccc} G_n & \xrightarrow{\varphi_\sigma} & G_n \\ \prod_{i \in I} \beta_i & \longmapsto & \varphi_\sigma \left(\prod_I \beta_i \right) \stackrel{\text{def.}}{=} \prod_I \beta_{\sigma(i)} \end{array}$$

φ_σ is an automorphism¹².

[Back to Proof: footnote 15](#)

[Back to Example 2: chapter IX on page 15](#)

[Back to Property 2 footnote 57 on page 22](#)

Let be $\sigma \in \text{Aut}(G_n)$ then the unique linear map associated with σ in the $\mathbb{F}_2$ -vector space $\mathbb{F}_2^n$ is bijective that is an element of the linear group $GL_n(\mathbb{F}_2)$, so $|\text{Aut}(G_n)|$ is exactly the order of linear group $GL_n(\mathbb{F}_2)$ which is: $\prod_{I_n} (2^n - 2^{k-1})$

$$|\text{Aut}(G_n)| = \prod_{I_n} (2^n - 2^{k-1}) \quad (1)$$

[Back to counting of code keys, “Game Strategy” in footnote 72 on page 32](#)

Let φ be an automorphism of G_n, H_1, H_2 , two subgroups of G_n , direct product of G_n ¹³, then G_n is a direct product of $\varphi(H_1)$ and $\varphi(H_2)$: $G_n = \varphi(H_1)\varphi(H_2)$ ¹⁴

$$G_{p+q} = HG_q \text{ with } H = \prod_{i=q+1}^{p+q} (1 + \beta_i), \quad p, q \in I_n, p + q = n$$

H is a subgroup of G_n isomorphic to G_p ¹⁵ and since $H \cap G_q = 1$, G_{p+q} is a direct product of G_q and H , henceforth:

G_{p+q} is isomorphic to $G_p \times G_q$.

As a consequence: [Back to “Elements on the solution” footnote 68 on page 29](#)

[Back to “Epilog”: chapter XIX on page 37](#)

* For any p in I_n , G_p is a subgroup of G_n , in particular $G_p \supset G_{p-1}$.

12

$$\prod_I \beta_i, \prod_J \beta_j \in G_n, I, J \in \mathcal{P}(I_n). \\ \varphi_\sigma \left(\prod_I \beta_i \right) \varphi_\sigma \left(\prod_J \beta_j \right) = \prod_{I+J} \beta_{\sigma(i)} = \varphi_\sigma \left(\prod_{I+J} \beta_i \right) = \varphi_\sigma \left(\prod_I \beta_i \prod_J \beta_j \right)$$

$$\varphi_\sigma \varphi_{\sigma^{-1}} = \varphi_1 = 1, 1 = \text{identity, so } \varphi_\sigma \text{ is bijective.}$$

13

$$\text{that is: } G_n = H_1 H_2 = H_2 H_1, H_1 \cap H_2 = 1 \text{ and for all } h_1 \in H_1, h_2 \in H_2, h_1 h_2 = h_2 h_1$$

14

$$s \in H_1, t \in H_2, \varphi(st) = \varphi(s)\varphi(t) \in \varphi(H_1)\varphi(H_2) \\ x \in \varphi(H_1) \cap \varphi(H_2) = \varphi(H_1 \cap H_2) = \varphi(1) = 1, x = 1.$$

15

Via the isomorphism φ_σ of chapter VI, restricted to H : $H \mapsto G_p$, where: $\sigma(i) = i - q$ for $i \in I_n \setminus I_q$

· $G_p \setminus G_{p-1} = \beta_p G_{p-1}$, $G_n = (1 + \beta_n)G_{n-1} = G_{n-1} + \beta_n G_{n-1}$ Back to equivalence P_1/P_o footnote 61 on page 23

Any subgroup of G_n is isomorphic to a G_p group with $p \in \llbracket 0, n \rrbracket$ (2)

16

Back to subgroup G' VI on page 10 Back to G vs τ footnote 76 on page 40

Back to subgroup G , chapter VI on page 9 Back to Theorem proof in footnote 67 on page 29

Back to “Back to case $n = 4$ ”: footnote 63 on page 26 Back to “Epilog”: chapter XIX on page 37

We denote: $\langle A \rangle$ or $\langle \gamma_i \rangle_I$ for $A \subset G_n$, $I \subset I_2^n$, $\gamma_i \in G_n$, the subgroup of G_n generated by $\{\gamma\}_A$, or respectively $\{\gamma_i\}_I$, thus:

$G_2 = \langle \beta_i \rangle_{I_2} = \langle \beta_1 + \beta_2 \rangle$, we will also write $\langle \beta_1, \beta_2 \rangle$ instead.

Division

$1 \neq \gamma \in G$ a subgroup of G_n then $G = (1 + \gamma)H$ where H a subgroup of G_n with $\gamma \notin H$ (3)

¹⁷Back to equivalence P_1/P_o footnote 61 on page 23

Now let's consider the permutation¹⁸ of G_n , Back to case $n = 5$ proof in footnote 2 on page 30

16

Let H be a non trivial subgroup of G_n generated by $(\gamma_i)_{I_h}$, $I_h \subset I_2^n$ ($h \neq 0$), $\gamma_i \neq 1$ for $i \in I_h$, this set being minimal for cardinal.

Let's prove first that $K, J \subset I_h$, if $\prod_J \gamma_i = \prod_K \gamma_i$ then $J = K$

Let be $K, J \subset I_h$, $J \neq K$, then $\prod_J \gamma_i \neq \prod_K \gamma_i$, otherwise $k \in K + J$, $\prod_J \gamma_i = \prod_K \gamma_i$ then $\prod_{(J+K) \setminus \{k\}} \gamma_i = \gamma_k$ and I_h would not be minimal.

Now consider:

$$I \subset I_h \quad \begin{array}{ccc} G_h & \xrightarrow{\varphi} & H \\ \prod_I \beta_i & \longmapsto & \prod_I \gamma_i \end{array}$$

φ is an isomorphism:

· φ is a morphism:

$$J, K \subset I_h, \quad \varphi\left(\prod_J \beta_i \prod_K \beta_i\right) = \varphi\left(\prod_{J+K} \beta_i\right) = \prod_{J+K} \gamma_i = \prod_J \gamma_i \prod_K \gamma_i = \varphi\left(\prod_J \beta_i\right) \varphi\left(\prod_K \beta_i\right)$$

· φ is surjective by design

· φ is injective:

Let's assume that $\varphi\left(\prod_J \beta_i\right) = \varphi\left(\prod_K \beta_i\right)$ that is: $\prod_J \gamma_i = \prod_K \gamma_i$ from what precedes $K = J$, hence $\prod_J \beta_i = \prod_K \beta_i$

17

Back to unicity, proof in footnote 3 on page 24

Let's denote $\gamma = \gamma_1, \gamma_2, \dots, \gamma_{|G|}$ the elements of G a non trivial subgroup of G_n ; $\Gamma_o = \emptyset$; and for $i \in I_{|G|}$

$$\begin{cases} \Gamma_i = \Gamma_{i-1} + \gamma_i & \text{if } \gamma_i \notin \Gamma_{i-1} + \gamma > \\ \Gamma_i = \Gamma_{i-1} & \text{otherwise} \end{cases}$$

Necessarily there's a p in $I_{|G|}$ for which: $G = \langle \Gamma_p + \gamma \rangle = (1 + \gamma) \langle \Gamma_p \rangle$.

$\gamma \notin \langle \Gamma_p \rangle$ otherwise:

$$\exists I \in \mathcal{P}(I_p), \gamma = \prod_I \gamma_i. \text{ Let } m \text{ be } \max(I), \gamma = \prod_{I \setminus \{m\}} \gamma_i \gamma_m, \prod_{I \setminus \{m\}} \gamma_i \in \langle \Gamma_{m-1} \rangle > (1 + \gamma),$$

$$\gamma m = \prod_{I \setminus \{m\}} \gamma_i \gamma \in \langle \Gamma_{m-1} \rangle > (1 + \gamma) \gamma = \langle \Gamma_{m-1} \rangle > (1 + \gamma) = \langle \Gamma_{m-1} + \gamma \rangle, \text{ impossible by construction.}$$

We posit $H = \langle \Gamma_p \rangle$ and we are finished.

¹⁸ Since $\varphi_\gamma^2 = 1$ (The identity), φ_γ is bijective.

$\gamma \in G_n$:

$$\varphi_\gamma: \begin{array}{ccc} G_n & \xrightarrow{\varphi_\gamma} & G_n \\ s & \longmapsto & \gamma s \end{array}$$

Property: $\varphi_\gamma^2 = 1$ [Back to The isometry group example 1, chapter IX on page 15](#)

(The identity) [Back to semidirect proof footnote 41 on page 17](#)

And then $\mathcal{P}(G_n)$ has a natural structure of $\mathcal{P}(G_n)$ -module on itself, the map:

$$\widetilde{\varphi}_\gamma: \begin{array}{ccc} \mathcal{P}(G_n) & \xrightarrow{\widetilde{\varphi}_\gamma} & \mathcal{P}(G_n) \\ A & \longmapsto & \varphi_\gamma(A) \end{array}$$

is $\mathcal{P}(G_n)$ -linear¹⁹. Indeed:

$$\cdot \quad \gamma \in G_n \quad A, B \in \mathcal{P}(G_n), \quad \varphi_\gamma(AB) = \varphi_\gamma(A)B \quad 20$$

In particular: $s \in G_n, \varphi_\gamma(s) = s\varphi_\gamma(1)$ [Back to semidirect proof footnote 41 on page 17](#)

[Back to unicity proof footnote 62 on page 24](#)

Remark: For $A \subset G_n$ we denote: $\mathbb{C}_A \stackrel{\text{def.}}{=} G_n \setminus A, \quad A, B \in \mathcal{P}(G_n), \gamma \in G_n, \gamma \mathbb{C}_A = \mathbb{C}_{\gamma A}, \gamma(A \cap B) = \gamma A \cap \gamma B,$

$\gamma(A \cup B) = \gamma A \cup \gamma B$.²¹ [Back to case = 5 proof in footnote 2 on page 30](#)

Now consider the projection, P^p (See footnote: ²²): $G_{p+q} \xrightarrow{P^p} G_p \times 1$, we have $\ker P^p \sim G_q \quad \text{Im} P^p \sim G_p$ denoting π^p the canonical projection on G_{p+q}/G_q , there's a unique isomorphism $\tilde{P}^p$ which renders the following commutative diagram:

$$\begin{array}{ccc} G_{p+q} & \xrightarrow{P^p} & G_p \times 1 \\ \pi^p \downarrow & & \uparrow \text{injection} \\ G_{p+q}/G_q & \xrightarrow{\tilde{P}^p} & G_p \end{array}$$

[Back to Proof: footnote 35 on page 14](#)

¹⁹

$A, B \in \mathcal{P}(G_n)$

· $\varphi_\gamma^2 = 1, \varphi_\gamma$ bijective: $\varphi_\gamma(A+B) = \varphi_\gamma(A \setminus B \cup B \setminus A) = \varphi_\gamma(A) \setminus \varphi_\gamma(B) \cup \varphi_\gamma(B) \setminus \varphi_\gamma(A) = \varphi_\gamma(A) + \varphi_\gamma(B)$

· $\varphi_\gamma(AB) = \varphi_\gamma(A)B$: see footnote: 20

²⁰

$$A = \sum_I a_i \quad B = \sum_J a_j \quad I, J \subset I_{2^n} \quad a_i \in G_n$$

$$\varphi_\gamma(\sum_{I \setminus J} a_i a_j) = \sum_{I \setminus J} \gamma a_i a_j = \varphi_\gamma(A)B \quad \text{Back to proof } \varphi_\gamma \text{ linear footnote 19}$$

²¹

²²

Since φ_γ permutation of G_n and $\varphi_\gamma(C) = \gamma C$ for any $C \in \mathcal{P}(G_n)$

If $k \in I_n \setminus I_q, P^p(\beta_k) = \beta_{k-q} \times 1_{G_q}$, equals to $1_{G_p} \times 1_{G_q}$ otherwise.

We also denote π_q the canonical projection on G_{p+q}/G_p corresponding to the projection P_q :

$$G_{p+q} \xrightarrow{P_q} 1 \times G_q.$$

Notations:

For (a, b) in $G_p \times G_q$, we will denote axb ; for $(1, b)$, $1xb$ or b . $r \in G_n$ we will write: $r = sxt$, $s \in G_p$, $t \in G_q$.

For $sxt \in G_p \times G_q$ and $k \in I_n$ we will denote: $\beta_k(sxt) = \beta_{k-q}sxt$ if $k \in I_n \setminus I_q$ and $\beta_k(sxt) = sx\beta_k t$ otherwise (indeed setting the isomorphism $\varphi: G_n \xrightarrow{\varphi} G_p \times G_q$).

We will identify $\pi^p(G_n)$ and G_p or $G_p \times 1_q$ (1_q the neutral of G_q); $\pi_q(G_n)$ and G_q . We will denote: $\pi^0, \pi_0: G_n \longrightarrow G_0 = \{1\}$; $a \in G_n$, $a = \pi^p(a) \times \pi_q(a)$.

[Back to Property 1 footnote 54 on page 21](#)

Properties:

• Since π_q homomorphism, $a, b \in G_n$, $\pi_q(ab) = \pi_q(a)\pi_q(b)$. in particular $axb \in G_p \times G_q$, $\pi_q(axb) = b$

Let G be a subgroup of G_n and ψ an isomorphism from G_p to G for a $p \in I_n$ well chosen (see proposition: 2 on page 7) .

We call η an automorphism of G_n , an embedding of G_n for ψ , if the restriction of η , to G_p equals to ψ that is: $\eta|_{G_p} = \psi$ with the following commutative diagram:

$$\begin{array}{ccc} G_n & \xrightarrow{\eta} & G_n \\ \text{injection} \uparrow & & \nearrow \psi \\ G_p & & \end{array}$$

See examples in the footnote: ²³[Back to proof in footnote: 41 on page 17](#)

23

$G = 1 + \beta_1\beta_2\beta_3$, $G_2G = G_3$ (Since $|G_2G| = 2.4 = 2^3$, $GG_2 \subset G_3$, $G_2G = G_3$).
 $\psi(1_2 \times G_1) = G$, η :

$$\begin{array}{ccccc} G_2 & \times & G_1 & \xrightarrow{\eta} & G_3 = G_2G \\ g & \times & \beta_1 & \mapsto & g\beta_1\beta_2\beta_3 \\ g & \times & 1 & \mapsto & g \end{array}$$

η is an isomorphism:

$g_1, g_2 \in G_2$

$$\eta(g_1\beta_1 \ g_2\beta_1) = \eta(g_1g_2) = g_1g_2 = \eta(g_1\beta_1)\eta(g_2\beta_1) \ / \ \eta(g_1\beta_1 \ g_2) = g_1g_2\beta_1\beta_2\beta_3 = \eta(g_1\beta_1)\eta(g_2) \ / \ \eta(g_1g_2) = g_1g_2 = \eta(g_1)\eta(g_2)$$

η has the announced property: by design $\eta|_{1_2 \times G_1} = \psi$

Hereunder another example: $G = 1 + \beta_1\beta_2$, $p = 1$

ψ	1	$\beta_1\beta_2$		
G_2	1	β_1	β_2	$\beta_1\beta_2$
η	1	$\beta_1\beta_2$	β_2	β_1

We have:

$$\begin{array}{llll} \eta(\beta_1\beta_2) = \beta_1 & \eta(\beta_1)\eta(\beta_2) = \beta_1\beta_2\beta_2 & \eta(\beta_2(\beta_1\beta_2)) = \beta_1\beta_2 & \eta(\beta_2)\eta(\beta_1\beta_2) = \beta_2\beta_1 \\ \eta(\beta_1(\beta_1\beta_2)) = \beta_2 & \eta(\beta_1)\eta(\beta_1\beta_2) = \beta_1\beta_2\beta_1 & \text{Thus } \eta \text{ is an embedding of } G_2 \text{ for } \psi & \end{array}$$

Property:

For any isomorphism ψ which sends G_p onto a subgroup G of G_n , we can construct an embedding η as above²⁴ and G_n is the direct product of G and G_q . [Back to \$G\$ vs \$\tau\$ footnote 76 on page 40](#)

[Back to case \$n = 4\$ footnote 63 on page 26](#) [Back to case \$n = 4\$ footnote 64 on page 26](#)

[Back to General case, footnote: 66 on page 28](#) [Back to Epilog in chapter XIX on page 37](#)

Now having an embedding η of G_n for such an isomorphism ψ , then η passes to the quotient, by defining: $\bar{\eta} \circ \pi_q = \pi_G \circ \eta$ ²⁵ with the following commutative diagram:

$$\begin{array}{ccc} G_n & \xrightarrow{\eta} & G_n \\ \pi_q \downarrow & & \downarrow \pi_G \\ G_n/G_p & \xrightarrow{\bar{\eta}} & G_n/G \end{array}$$

$\bar{\eta}$ is an isomorphism²⁶ [Back to footnote 63 on page 26](#) [Back to case \$n = 4\$ in footnote 63 on page 26](#)

24

G = subgroup of G_n , we denote π_G the canonical projection onto G_n/G .

Let's choose a lift $\widetilde{\pi}_G$ of π_G such that $\widetilde{\pi}_G(1) = 1$. So we have: $\pi_G \circ \widetilde{\pi}_G = 1$

We denote $\bar{\gamma} = \gamma G$ the class of $\gamma \in G_n$. $G_n/G = \langle \bar{\beta}_i \rangle_K$, $K \in \mathcal{P}(I_n)$ minimal for cardinal.

We posit: $\widetilde{\beta}_i = \widetilde{\pi}_G(\bar{\beta}_i)$ for $i \in K$, then we define the map, $v: G_n/G \longrightarrow G_n$ by: $v(\prod_I \bar{\beta}_i) = \prod_I \widetilde{\beta}_i$, for $I \subset K$

· v is a morphism:

$$\alpha = \prod_I \bar{\beta}_i, \beta = \prod_J \bar{\beta}_j \quad I, J \subset K,$$

$$v(\alpha\beta) = v(\prod_{I+J} \bar{\beta}_i) = \prod_{I+J} \widetilde{\beta}_i = \prod_I \widetilde{\beta}_i \prod_J \widetilde{\beta}_j = v(\alpha)v(\beta), \text{ since for } i = j \in I_n, \widetilde{\beta}_i \widetilde{\beta}_j = \widetilde{\beta}_i^2 = 1 \text{ see in chapter III on page 3}$$

· $\pi_G \circ v = 1$:

$$\pi_G \circ v(\alpha) = \pi_G \circ v(\prod_I \bar{\beta}_i) = \pi_G(\prod_I \widetilde{\beta}_i) = \pi_G(\prod_I \widetilde{\pi}_G(\bar{\beta}_i)) = \prod_I \pi_G \circ \widetilde{\pi}_G(\bar{\beta}_i) = \prod_I \bar{\beta}_i = \alpha.$$

Now consider the short exact sequence: $1 \longrightarrow G_p \xrightarrow{\psi} G_n \xrightarrow{\pi_G} G_n/G \longrightarrow 1$ where ψ is an isomorphism from G_p to G , $p \in I_n$.

v is a split for the above sequence, so G_n is a semidirect product of G and G_n/G and G being abelian:

$G_n \sim G \times G_n/G$ then $1 \times G_n/G$ is a subgroup of G_n isomorphic to G_q since the index of G in G_n is q ($n = p + q$) hence $G_n \sim G \times G_q$.

Now consider the map:

$$\varphi: \begin{array}{ccc} G_p & \times & G_q \\ (s & \times & t) \end{array} \xrightarrow{\psi \times 1} G \times G_q \sim G_n$$

It is a surjective morphism, so $\eta = \psi \times 1$ is an automorphism of G_n , which verifies: $\eta|_{G_p} = \psi$, it is an embedding of G_n for ψ .

25

$\bar{\eta}$ is well defined:

$a, b \in G_n$ with $a = gb$, $g \in G_p$

We have: $\pi_G \circ \eta(a) = \pi_G \circ \eta(g)\pi_G \circ \eta(b) = \pi_G \circ \psi(g)\pi_G \circ \eta(b) = \pi_G \circ \eta(b)$

It is a morphism:

$a, b \in G_n$ with $a = \pi_q(a')$, $b = \pi_q(b')$

$$\bar{\eta}(ab) = \pi_G \circ \eta(a'b') = \pi_G \circ \eta(a')\pi_G \circ \eta(b') = \bar{\eta}(a)\bar{\eta}(b)$$

26

Since η bijection, $\pi_G \circ \eta = \bar{\eta} \circ \pi_q$ is surjective, $\bar{\eta}$ is surjective. Now $|G_n/G| = |G_n/G_p|$, so $\bar{\eta}$ is a bijection.

Now consider two subgroups of G_n , G and G' with $|G| \geq |G'|$ according to statement 2 on page 7 we have an isomorphism ψ which maps G' to a subgroup of G , then we have an embedding η with the following commutative diagram: [Back to unicity proof footnote 62 on page 24](#)
[Back to unicity proof item 5. footnote 62 on page 25](#) [Back to proof property 4, footnote 59 on page 23](#)

$$\begin{array}{ccc} G_n & \xrightarrow{\eta} & G_n \\ \text{injection} \uparrow & & \nearrow \psi \\ & G' & \end{array}$$

And then η passes to the quotient with the isomorphism $\bar{\eta}$ defined by: $\bar{\eta} \circ \pi_{G'} \stackrel{\text{def.}}{=} \pi_{\eta(G')} \circ \eta$ ²⁷ and with the following commutative diagram:
[Back to subgroup \$G'\$ proof footnote 59 on page 23](#) [Back to “ \$\Omega\$ to quotient” footnote 76 on page 40](#)

$$\begin{array}{ccc} G_n & \xleftarrow{\eta} & G_n \\ \pi_{\eta(G')} \downarrow & & \downarrow \pi_{G'} \\ G_n / \eta(G') & \xleftarrow{\bar{\eta}} & G_n / G' \end{array}$$

27

Let $a, b \in G_n$,

- $a = bg' \quad g' \in G', \bar{\eta} \circ \pi_{G'}(bg') = \pi_{\eta(G')} \circ \eta(b) \pi_{\eta(G')} \circ \eta(g') = \bar{\eta} \circ \pi_{G'}(b) \bar{\eta} \circ \pi_{G'}(g') = \bar{\eta} \circ \pi_{G'}(b)$
- $\bar{\eta} \circ \pi_{G'}(ab) = \pi_{\eta(G')} \circ \eta(a) \pi_{\eta(G')} \circ \eta(b) = \bar{\eta} \circ \pi_{G'}(a) \bar{\eta} \circ \pi_{G'}(b)$
- $\bar{\eta} \circ \pi_{G'} = \pi_{\eta(G')} \circ \eta$ is surjective, hence $\bar{\eta}$ an isomorphism.

VII A distance on G_n

Let be $s, t \in G_n$ we define the distance d_n on G_n by:

Let $J \subset I_n$ be the unique J (see Property in chapter III on page 3) such that $\prod_J \beta_i = st$,

$$d_n(s, t) \stackrel{\text{def.}}{=} |J|$$

28

We define: $\text{supp}_{\text{def.}} \gamma = J \in \mathcal{P}(I_n)$, the support of $\gamma = \prod_J \beta_i$ [Back to Proof: footnote 54 on page 21](#)

Properties:

$m, r \in G_q \quad s, t, \sigma \in G_n$

- $d_n(s, t) = 1 \iff \exists \beta \in \mathbb{B}_n$ such that: $s = \beta t$
- $d_n(\sigma s, \sigma t) = d_n(s, t)$
- $d_n(\sigma s, t) = d_n(s, \sigma t)$
- $d_n(r, m) = d_q(r, m)$

Consequence: There's no triangle in G_n .²⁹

We define: $s \in G_n, A \subset G_n \quad d_n(s, A) \stackrel{\text{def.}}{=} \min_{g \in A} d_n(s, g)$

[Back to semidirect proof footnote 41 on page 17](#)

We define for $\gamma \in G_n$: $\deg(\gamma) \stackrel{\text{def.}}{=} d_n(\gamma, 1)$, the degree of γ .

Properties:

- $s, t \in G_n, d_n(s, t) = d_n(st, 1) = \deg(st)$
- $\gamma \in G_n, \sigma \in \mathcal{T}(I_n), \deg(\varphi_\sigma(\gamma)) = \deg(\gamma)$ ³⁰
[Back to \$\sigma_n^p\$ properties footnote VIII on page 15/](#) [Back to semidirect proof footnote 41 on page 17](#)

28

- d_n is well defined, since G_n is a group and J unique.
- $d_n \in \mathbb{R}_+ \quad (d_n \in \llbracket 0, n \rrbracket)$
- for $s \in G_n \quad d_n(s, s) = |\emptyset| = 0$
 $s, t \in G_n$ if $d_n(s, t) = 0, st = 1$ by definition, $s = t$
- d_n is symmetric since G_n is commutative
- $st = \prod_J \beta_i, \quad tr = \prod_K \beta_i \in G_n \rightsquigarrow sr = \prod_{J+K} \beta_i \quad ; \quad J, K \in I_n$
 $|J+K| \leq |J| + |K|$
 $d_n(s, r) \leq d_n(s, t) + d_n(t, r)$

29

that is: there are no $s, t, r \in G_n$ distinct, with $d_n(s, t) = 1 \quad d_n(s, r) = 1 \quad d_n(r, t) = 1$. Proof:

Let be $s, t, r \in G_n$ with the property in question, $st = \beta \in \mathbb{B}_n, sr = \gamma \in \mathbb{B}_n$, then $stsr = tr = \beta\gamma \in \mathbb{B}_n$, but $|\text{supp}\beta\gamma| = 2$, absurd.

30

$$\deg(\gamma) = |\text{supp}\gamma|, \deg(\varphi_\sigma(\gamma)) = |\text{supp}\varphi_\sigma(\gamma)| = |\sigma(\text{supp}\gamma)| = |\text{supp}\gamma|$$

$$\cdot \alpha, \gamma \in G_n, \deg(\alpha) \neq \deg(\gamma) \implies \alpha \neq \gamma$$

31

Product distance

Back to existence theorem, consequences in footnote 67 on page 29

A, B being two metric spaces of distances d_A, d_B the product distance:

$$d_{A \times B}(a \times b, c \times d) = d_A(a, c) + d_B(b, d) \quad a, c \in A, b, d \in B \quad \text{on } A \times B \text{ is a distance}^{32}.$$

So for $p, q \in I_n$ on $G_p \times G_q$ we have the product distance that we denote $d_{p \times q}$:

$$s_1 \times t_1, s_2 \times t_2 \in G_p \times G_q \quad d_{p \times q}(s_1 \times t_1, s_2 \times t_2) = d_p(s_1, s_2) + d_q(t_1, t_2)$$

This distance coincides with the one on G_{p+q} :³³

$$s, t \in G_{p+q}, \quad G_{p+q} \stackrel{\varphi}{\sim} G_p \times G_q \quad d_{p+q}(s, t) = d_{p \times q}(\varphi(s), \varphi(t))$$

Hence φ is an isometry. (see definition in chapter IX on page 15)

So we will write $d_{p+q}(s_1 \times t_1, s_2 \times t_2) = d_p(s_1, s_2) + d_q(t_1, t_2)$

This distance passes to the quotient.

³¹ i.e. $\alpha = \gamma \implies \deg(\alpha) = \deg(\gamma)$

³²

$$\cdot d_{A \times B} \in \mathbb{R}_+, d_{A \times B} \text{ is symmetric}$$

$$\cdot d_{A \times B}(c, c') = 0 \implies c = c' \quad c, c' \in A \times B$$

$$d_{A \times B}(c, c) = 0 \quad c \in A \times B$$

$$\cdot a, a', a'' \in A \quad b, b', b'' \in B$$

$$\begin{aligned} d_{A \times B}(a \times b, a' \times b') &= d_A(a, a') + d_B(b, b') \\ &\leq d_A(a, a'') + d_A(a'', a') + d_B(b, b'') + d_B(b'', b') \\ &\leq d_{A \times B}(a \times b, a'' \times b'') + d_{A \times B}(a'' \times b'', a' \times b') \end{aligned}$$

33

$$G_{p+q} \stackrel{\varphi}{\sim} G_p \times G_q \quad I \subset I_n \setminus I_q, J \subset I_q \quad s = \prod_I \beta_i \prod_J \beta_i. \quad d_{p+q}(s, 1) = |I| + |J|$$

$$\sigma \text{ injection : } I_{p+q} \setminus I_q \xrightarrow{\text{def.}} I_p \quad \sigma(q+i) = i$$

$$\varphi(s) = \prod_I \varphi(\beta_i) \prod_J \varphi(\beta_i) = \left(\prod_{\sigma(I)} \beta_{\sigma(i)} \times 1 \right) \left(\prod_J 1 \times \beta_i \right) = \left(\prod_{\sigma(I)} \beta_{\sigma(i)} \right) \times \left(\prod_J \beta_i \right)$$

$$d_{p \times q}(\varphi(s), 1 \times 1) = d_p\left(\prod_{\sigma(I)} \beta_{\sigma(i)}, 1\right) + d_q\left(1, \prod_J \beta_i\right) = |\sigma(I)| + |J| = |I| + |J| = d_{p+q}(s, 1)$$

Now : $s_i \in G_p, t_i \in G_q$, for $i = 1, 2$

$$d_{p \times q}((s_1 \times t_1)(s_2 \times t_2), 1 \times 1) = d_{p \times q}(s_1 s_2 \times t_1 t_2, 1 \times 1) = d_p(s_1 s_2, 1) + d_q(t_1 t_2, 1) = d_p(s_1, s_2) + d_q(t_1, t_2) = d_{p \times q}(s_1 \times t_1, s_2 \times t_2)$$

from above:

$$d_{p \times q}((s_1 \times t_1)(s_2 \times t_2), 1 \times 1) = d_{p+q}(\varphi^{-1}((s_1 \times t_1)(s_2 \times t_2)), 1) = d_{p+q}(\varphi^{-1}(s_1 \times t_1) \varphi^{-1}(s_2 \times t_2), 1) = d_{p+q}(\varphi^{-1}(s_1 \times t_1), \varphi^{-1}(s_2 \times t_2))$$

the end of proof.

Quotient distance $\tilde{d}^p$: $s, t \in G_n \quad \tilde{d}^p(\pi^p(s), \pi^p(t)) = \min_{\text{def. } g \in G_q} d_{p+q}(gs, t)$ ³⁴

Nota: $\tilde{d}^p(\pi^p(s), \pi^p(t)) = \min_{\text{def. } g_1, g_2 \in G_q} d_{p+q}(g_1 s, g_2 t)$ is equivalent to the above.

property: $\tilde{d}^p(\pi^p(s), \pi^p(A)) = d_p(\tilde{P}^p \circ \pi^p(s), \tilde{P}^p \circ \pi^p(A))$ for $s \in G_{p+q}$ and $A \subset G_{p+q}$ ³⁵

This distance corresponds to d_p on $G_p \sim G_{p+q}/G_q$, since according to property above:
 $\tilde{d}^p(\pi^p(s), \pi^p(t)) = d_p(\tilde{P}^p \circ \pi(s), \tilde{P}^p \circ \pi(t)) = d_p(P^p(s), P^p(t))$

Similarly we denote $\tilde{d}_q$ stemming from $\tilde{P}_q$, with the same terminology.

More generally, having a subgroup G of G_n , and the canonical homomorphism projection:
 $\pi_G: G_n \longrightarrow G_n/G$ (since G_n is abelian, G is normal), we pass the distance d_n to the quotient by defining:
 $\tilde{d}(\pi_G(a), \pi_G(b)) = \min_{\text{def. } \gamma \in G} d_n(\gamma a, b)$ for $a, b \in G_n$, the proof is similar to the one in footnote 34.

VIII A partition of G_n by degrees

Now let's have a look at the polynomial $P \in \mathcal{P}(G_n)[X]$, defined by: $P = \prod_{I_n} (X + \beta_p) = \sum_{p=0 \text{ to } n} \sigma_{n-p}^n X^p$.

Which then defines $\sigma_p^n \in \mathcal{P}(G_n)$ for $p = 0, \dots, n$.

σ_p^n is the subset of the elements of G_n of degree p , $|\sigma_p^n| = \binom{n}{p}$ and $(\sigma_p^n)_{p=0 \text{ to } n}$ is a $(n+1)$ -partition of G_n ,
in particular $A \subset G_n \quad A = \sum_{p=0 \text{ to } n} A \cap \sigma_p^n$. [Back to proof in footnote: 41 on page 17](#)

34

quotient distance:

$\tilde{d}^p$ is a distance:

- It is well defined: it doesn't depend on the s and t chosen for the class $\pi^p(s)$ and $\pi^p(t)$.
- $\tilde{d}^p \in \mathbb{R}_+$
- for $s, t \in G_{p+q} \quad \tilde{d}^p(\pi^p(s), \pi^p(t)) = 0$, there exists $g \in G_q \quad d_{p+q}(gs, t) = 0, gs = t$ that is $\pi^p(s) = \pi^p(t)$
 $\tilde{d}^p(s, s) = \min_{g \in G_q} d_{p+q}(gs, s) = d_{p+q}(s, s) = 0$
- $\tilde{d}^p$ is symmetric since d_{p+q} is.
- $g_1, g_2 \in G_q \quad s, t, r \in G_{p+q}$

$$\begin{aligned} d_{p+q}(g_1 s, g_2 t) &\leq d_{p+q}(g_1 s, r) + d_{p+q}(r, g_2 t) \\ \min_{g_1, g_2 \in G_q} d_{p+q}(g_1 s, g_2 t) &\leq \min_{g_1, g_2 \in G_q} (d_{p+q}(s, g_1 r) + d_{p+q}(r, g_2 t)) \\ &\leq \min_{g \in G_q} (d_{p+q}(s, gr)) + \min_{g \in G_q} (d_{p+q}(r, gt)) \end{aligned}$$

35

Proof:

$s \sim s_1 x s_2 \in G_p \times G_q$

$t \sim t_1 x t_2 \in G_p \times G_q, t \in A$

$$\begin{aligned} \min_{g \in G_q} d_{p+q}(s, gt) &= d_p(s_1, t_1) + \min_{g \in G_q} d_q(1, s_2 t_2 g) \\ &= d_p(s_1, t_1) \\ \tilde{d}^p(\pi^p(s), \pi^p(A)) &= \min_{t_1} d_p(s_1, t_1) \\ &= d_p(\tilde{P}^p \circ \pi^p(s), \tilde{P}^p \circ \pi^p(A)) \text{ see diagram in chapter VI on page 8} \end{aligned}$$

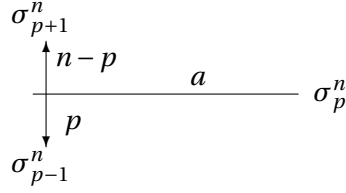
Example: for $n = 3$, $\sigma_3^3 = \beta_1\beta_2\beta_3$, $\sigma_1^3 = \beta_1 + \beta_2 + \beta_3$, $\sigma_o^n = 1$, $\sigma_1^n = \mathbb{B}_n$

Definition: $a, b \in G_n$ are linked if $\deg(ab) = 1$

And so if $a, b \in G_n$ are linked, there exists $\beta \in \mathbb{B}_n$ such that $a = \beta b$. β is unique since G_n is a group, and we will call elements of $\mathbb{B}_n$, links. [Back to proof in footnote: 41 on page 17](#)

Properties 2:

- $a \in \sigma_p^n$, There are exactly $n - p$ elements of σ_{p+1}^n , and exactly p elements of σ_{p-1}^n linked to a . Those are the only links to a .³⁶ As a consequence: a belonging to σ_p^n is linked exactly to n elements and they all belong to σ_{p+1}^n or σ_{p-1}^n . (see the following diagram): [Back to Proof: footnote 50 on page 20](#)



- $\varphi_\sigma(\sigma_p^n) = \sigma_p^n$ $\sigma \in \mathcal{T}(I_n)$ ³⁷

IX The isometric group $\mathcal{I}_{\text{som}}$

[Back to product distance: chapter VII on page 13](#) [Back to filling out the board: footnote 75 on page 34](#)
[Back to unicity, proof in footnote 62 on page 25](#)

Let $(G, d), (G', d')$ be metric groups $\psi: G \longrightarrow G'$, a bijective map. We say that ψ is an isometry, if:
 $\forall_{G \times G'}(s, t) \quad d(s, t) = d'(\psi(s), \psi(t))$

We say that ψ is an isometry of G , when $G = G'$ Properties:

- The set of isometries of G_n altogether with the law of composition of mappings, is a group.³⁸

We will call $\mathcal{I}_{\text{som}_n}$ the set of isometries of G_n , or $\mathcal{I}_{\text{som}}$ if there's no ambiguity.

Remark: Since $\mathcal{I}_{\text{som}} \subset \mathcal{T}(G_n)$, the permutations of G_n , it is a finite group.

Example 1: φ_γ defined in chapter VI on page 7.

Example 2: φ_σ defined in chapter VI on page 6 is also an isometry.

³⁶

$a = \prod_I \beta_i \in G_n$, with $I \in \mathcal{P}(I_n) \quad |I| = p$,
 $b \in G_n$ with $\deg(ab) = 1$, $b = a\beta_i$, either $i \in I_n \setminus I$ (occurrence: $|I_n \setminus I| = n - p$), $\deg b = p + 1$; or $i \in I$ (occurrence $|I| = p$), $\deg b = p - 1$

³⁷

For $\gamma \in G_n$, $\deg(\varphi_\sigma(\gamma)) = \deg(\gamma)$ (see in chapter VII on page 12)

³⁸

The set of bijective maps with the law in question is a group. φ, ψ , bijective maps, two isometries, for every t, s belonging to G_n ,
 $d_n(\varphi \circ \psi(t), \varphi \circ \psi(s)) = d_n(\psi(s), \psi(t)) = d_n(s, t)$. So, the set of isometries is a sub-group of the bijective maps, thus a group.

Back to Property 2 footnote 57 on page 22

We denote:

- $G_\gamma = \{\varphi_\gamma \text{ for } \gamma \in G_n\}$
- $G_\sigma = \{\varphi_\sigma \text{ for } \sigma \in \mathcal{T}(I_n)\}$, $\mathcal{T}(I_n)$ the permutations of I_n

Properties:

- $\varphi \in \mathcal{S}\text{om}$ means that for any $(\alpha, \beta) \in G_n^2$, $\deg(\varphi(\alpha)\varphi(\beta)) = \deg(\alpha\beta)$
- G_γ is an abelian subgroup of the group $\mathcal{S}\text{om}$ isomorphic to G_n ³⁹
- G_σ is a subgroup of the group $\mathcal{S}\text{om}$ isomorphic to $\mathcal{T}(I_n)$ ⁴⁰

39

Actually, G_γ is the image of G_n by the homomorphism :

$$\begin{array}{ccc} \varphi: & G_n & \xrightarrow{\varphi} \mathcal{S}\text{om} \\ & \gamma & \longmapsto \varphi_\gamma \end{array}$$

Back to Notations for elements of G_γ footnote IX on page 18

so it is a subgroup of $\mathcal{S}\text{om}$. Proof that φ is a homomorphism: $\alpha, \beta \in G_n \quad \varphi(\alpha\beta) = \varphi_\alpha\beta = \varphi_\alpha \circ \varphi_\beta = \varphi(\alpha) \circ \varphi(\beta)$
Also φ is injective since for $\varphi(\gamma) = 1$ (identity) in particular $\varphi_\gamma(1) = 1$ that is $\gamma = 1$ and then the image G_γ is isomorphic to G_n .
 G_n being abelian, G_γ is also.

Nota:

$$\begin{array}{ccc} \varphi^{-1}: & G_\gamma & \xrightarrow{\varphi^{-1}} G_n \\ & \varsigma & \longmapsto \varsigma(1) \end{array}$$

40

G_σ is the image of $\mathcal{T}(I_n)$ by the homomorphism :

$$\begin{array}{ccc} \xi: & \mathcal{T}(I_n) & \xrightarrow{\xi} \mathcal{S}\text{om} \\ & \sigma & \longmapsto \varphi_\sigma \end{array}$$

So it is a subgroup of $\mathcal{S}\text{om}$. Proof that ξ is a homomorphism: $\alpha, \beta \in \mathcal{T}(I_n) \quad \xi(\alpha\beta) = \varphi_\alpha\beta = \varphi_\alpha \circ \varphi_\beta = \xi(\alpha) \circ \xi(\beta)$
Also ξ is injective since for $\xi(\sigma) = 1$ (identity) in particular $\varphi_\sigma(\beta_i) = \beta_i$ that is $\sigma(i) = i$ for all $i \in I_n$ and the image G_σ is isomorphic to $\mathcal{T}(I_n)$.

· $\mathcal{I}\text{som}$ is the semidirect product of G_γ and G_σ , $\mathcal{I}\text{som} = G_\gamma \ltimes G_\sigma$ ⁴¹

· the injective homomorphism:⁴²

$$\varphi: \begin{array}{ccc} G_n & \xrightarrow{\varphi} & \mathcal{T}(\mathcal{P}(G_n)) \\ \gamma & \longmapsto & \varphi_\gamma \end{array}$$

Defines an action onto $\mathcal{P}(G_n)$:

$$\begin{array}{ccc} G_n \times \mathcal{P}(G_n) & \longrightarrow & \mathcal{P}(G_n) \\ (\gamma, A) & \longmapsto & \gamma A = \varphi_\gamma(A) \end{array}$$

And so G_n acts faithfully on $\mathcal{P}(G_n)$ and for example we have:

41

· $G_\sigma \cap G_\gamma = \{1\}$:

$s \in G_n$, $\varphi \in G_\gamma \cap G_\sigma$, $\varphi(\varphi(1)) = \varphi^2(1) = 1$ according to VI on page 8, $\deg(\varphi(1)) = 0$ according to chapter VII on page 12, $\varphi(1) = 1$, $\varphi(s) = s\varphi(1) = s$, according to VI on page 8, $\varphi = 1$

· $\mathcal{I}\text{som} = G_\gamma \circ G_\sigma$:

Let be $\zeta \in \mathcal{I}\text{som}$, for $(\alpha, \beta) \in G_n^2$ we have: $\deg(\zeta(\alpha)\zeta(\beta)) = \deg(\alpha\beta)$, let's denote: $\varphi' \stackrel{\text{def}}{=} \varphi(\zeta(1))$

Because $\varphi' \circ \zeta$ is an isometry we have also $\deg(\varphi' \circ \zeta(\alpha)\varphi' \circ \zeta(\beta)) = \deg(\alpha\beta)$. With $\beta = 1$, it comes: $\deg(\varphi' \circ \zeta(\alpha)) = \deg(\alpha)$, since $\varphi' \circ \zeta(1) = \varphi_{\zeta(1)}(\zeta(1)) = 1$

$\varphi' \circ \zeta$ leaves $\sigma_1^n = \mathbb{B}_n$ unchanged (And also any σ_n^p by the way), it is then a permutation of $\mathbb{B}_n$, so there exists $\sigma \in \mathcal{T}(I_n)$ such that: $\varphi_\sigma \circ \varphi' \circ \zeta(\beta_i) = \beta_i$ for all $i \in I_n$, notice that $\varphi_\sigma \circ \varphi' \circ \zeta(1) = 1$, remark also that since φ_σ leaves the degree unchanged $\varphi_\sigma \circ \varphi' \circ \zeta$ also.

Let's prove by induction on p that the restriction of $\psi \stackrel{\text{def}}{=} \varphi_\sigma \circ \varphi' \circ \zeta$ to σ_p^n is the identity:

· For $p = 1$ that's true.

· Assuming the property to be true up to $p \in I_n$, we have for any $I \subset I_n$ with $|I| = p + 1$, $i, j \in I$ $i \neq j$, denoting $\beta \in G_n$ whose $\text{supp}\beta = I$:

$\psi(\beta)\beta\beta_i = \psi(\beta)\psi(\beta\beta_i)$ is of degree of β_i equal to 1, let's say that $\psi(\beta)\beta\beta_i = \beta_k$ for a $k \in I_n$, equally we have:

$\psi(\beta)\beta\beta_j = \beta_{k'}$ for a $k' \in I_n$ which leads to:

$\beta_i\beta_j = \beta_k\beta_{k'}$

either $\beta_k = \beta_i$, $\beta_{k'} = \beta_j$, hence $\psi(\beta)\beta = 1$, $\psi(\beta) = \beta$

or else $\beta_k = \beta_j$, $\beta_{k'} = \beta_i$, $\psi(\beta)\beta\beta_i = \beta_j$, $\psi(\beta) = \beta\beta_i\beta_j$, though $\psi(\beta)$ is of degree $p + 1$ and $\beta\beta_i\beta_j$ of degree $p - 1$ which is impossible. The end of the proof.

So $\{\sigma_p^n\}_{p=0 \text{ to } n}$ being a partition of G_n (see in chapter VIII on page 14), $\zeta = \varphi' \circ \varphi_{\sigma^{-1}}$, $\mathcal{I}\text{som} = G_\gamma \circ G_\sigma = G_\sigma \circ G_\gamma$

· G_γ is normal:

$\sigma \in G_\sigma$, $\zeta, \zeta' \in G_\gamma$, $h \in G_n$, $(\sigma\zeta')\zeta(\zeta'\sigma^{-1}) = \sigma\zeta\sigma^{-1}$

$\sigma\zeta\sigma^{-1}(h) = \sigma(\sigma^{-1}(h)\zeta(1)) = h\sigma(\zeta(1))$, $\sigma\zeta\sigma^{-1} = \varphi(\sigma\zeta(1)) \in G_\gamma$

42

· It is a homomorphism:

$\gamma_1, \gamma_2 \in G_n$, $\varphi_{\gamma_1} \circ \varphi_{\gamma_2} = \varphi_{\gamma_1\gamma_2}$

· it is injective: $\mathcal{Ker}\varphi = \{\gamma \in G_n, \varphi_\gamma = 1\}$

$\varphi_\gamma \in \mathcal{Ker}\varphi$, $\varphi_\gamma = 1$, in particular $1 = \varphi_\gamma(1) = \gamma$.

$|G_n| = |\text{stabilizer}_A^n| \cdot |\text{orbit}_A^n|_{\mathcal{P}(G_n)}$ for $A \in \mathcal{P}(G_n)$ ⁴³. That is the length of the orbit of A equals to the index in G_n of the stabilizer of A , in other terms: $\text{orbit}_A^n \sim G_n / G$, where $G \stackrel{\text{def.}}{=} \text{stabilizer}_A^n$

Back to case $n = 8$ in footnote 65 on page 27 Back to “property 4” in footnote 59 on page 23

Nota: For $\gamma \in G_n$, and $A \in \mathcal{P}(G_n)$, we have, (group action) $\gamma A = \varphi_\gamma(A) = \gamma A$ (operation in the module $\mathcal{P}(G_n)$ on itself).

Notations:

Now for $\varsigma \in \mathcal{I}_{\text{som}}$ we can also construct an action onto $\mathcal{P}(G_n)$ (definition: $\varsigma A = \varsigma(A)$), and so, in the following we will write: ςA instead of $\varsigma(A)$.

$A \in \mathcal{P}(G_n)$, G its stabilizer (see footnote: 43 for a definition), remarks:

Back to Property 2 in footnote 57 on page 22

$$\cdot GA = A \iff GA \subset A$$

· If $1 \in A$, then $G \subset A$ ⁴⁴ Back to proof on solution P_1 in footnote 58 on page 22 Back to Property 4 footnote 59 on page 23

X The γ -core of G_n

Definition :

$A \in \mathcal{P}(G_n)$, $\gamma \in G_n$

Back to Epilog, chapter XIX on page 37

· We say that A is a γ -core if it is stable by φ_γ (i.e. $\varphi_\gamma A \subset A$)
If A is a γ -core, $\varphi_\gamma A = A \iff (1 + \gamma)A = \emptyset$

XI The property P_o

Let P_o be the following property for a **non empty** set $A \in \mathcal{P}(G_n)$,

$$P_o: \quad \forall s \in G_n \quad d_n(A \setminus s, s) = 1$$

In terms of n -cube $G_n \sim \mathbb{F}_2^n$ this means for any vertex s in $\mathbb{F}_2^n$ there exists an edge linking it to a vertex in A .

We will also later on use the weaker version of P_o :

$$P_1: \quad \forall s \in G_n \quad d_n(A, s) \leq 1$$

Example, see figure: 2 on the next page.

⁴³

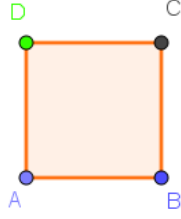
$\text{stabilizer}_A^n \stackrel{\text{def.}}{=} \{\gamma \in G_n / \gamma A = A\}$, it is a subgroup of G_n
 $\text{orbit}_A^n \stackrel{\text{def.}}{=} \{B \in \mathcal{P}(G_n) / \exists \gamma \in G_n \quad B = \gamma A\}$

Back to remarks chapter IX

⁴⁴

$1 \in A$ thus $G1 = G \subset A$

Figure 2: The properties P_o and P_1 for $n = 2$



$\{A, B\}$ with property P_o
 $\{D\}$ without
 $\{A, C\}$ with property P_1

Properties:

[Back to “Miscellaneous” XIII on page 28](#)

- $A \in \mathcal{P}(G_n)$ possesses the property P_o means that any element of G_n has a link to A .
- $A \in \mathcal{P}(G_n)$ possesses the property P_1 means that any element of $G_n \setminus A$ has a link to A .
- $P_o \implies P_1$ [Back to General case \$n\$ footnote 66 on page 28](#)
- φ isometry, $A \in \mathcal{P}(G_n)$ satisfying P_o (respectively P_1), then φA satisfies P_o (respectively P_1),
 In particular: $G_{p+q} \stackrel{\varphi}{\sim} G_p \times G_q$, φA satisfies P_o (P_1)⁴⁵ [Back to proof footnote 57 on page 22](#)
- if $A \in \mathcal{P}(G_n)$ satisfying P_1 is a β_i -core ($i \in I_n$) then A satisfies P_o ⁴⁶
[Back to proof footnote 54 on page 21](#) [Back to Remarks footnote 57 on page 22](#)
- $A \in \mathcal{P}(G_n)$ satisfying P_o , if $a \in A$ then $a \in \beta$ -core for a $\beta \in \mathbb{B}_n$ ⁴⁷

$A, B \subset G_n$ non empty subsets of G_n , A complying with P_1 then:

$$\text{If } B \supset A \text{ then } B \text{ satisfies } P_1 \quad (4)$$

⁴⁸ [Back to Remarks chapter XII on page 21](#)

⁴⁵

- Case P_1 : $\forall s \in G_n \quad d_n(A, \varphi^{-1}s) \leq 1, d_n(\varphi A, s) \leq 1$
- Case P_o : $\forall s \in G_n \quad d_n(A \setminus \varphi^{-1}s, \varphi^{-1}s) = 1, d_n(\varphi A \setminus s, s) = 1$

⁴⁶

For $s \in A \quad \varphi_{\beta_i}s \in A$ and $d_n(s, \varphi_{\beta_i}s) = d_n(\beta_i, 1) = 1$ and in particular $\varphi_{\beta_i}s \in A \setminus s$

⁴⁷

$a \in A$ has one link to A , so there is a $\beta \in \mathbb{B}_n$ such that $\beta a \in A$ that is $\varphi_\beta(a) \in A$

⁴⁸

$\forall s \in G_n, d_n(A, s) \leq 1$ then a fortiori $d_n(B, s) \leq 1$

$$\pi_q(A), \pi^P(A) \text{ comply with } P_1 \quad (5)$$

⁴⁹ Back to proof in footnote 54 on the following page Back to unicity, proof in footnote 3 on page 24
Back to equivalence P_1/P_o , proof in footnote 61 on page 23

XII Some G_n partitions

Let k be a non null integer lower than $|G_n|$. We call a k -set of $\mathcal{P}(G_n)$, a disjoint set family of $\mathcal{P}(G_n)$ composed of k non empty subsets of G_n . We say that k is the size of the k -set.

We say that the k -set $(A_i)_{I_k}$ of $\mathcal{P}(G_n)$ is a partition if $\sum_{I_k} A_i = G_n$.

We say that $(A_i)_{I_k}$ a set family of $\mathcal{P}(G_n)$ “satisfies or complies with P_1 ” (respectively P_o) if it is a k -set of $\mathcal{P}(G_n)$ for which for each set A_i , P_1 (respectively P_o) holds.

We will call a set family which complies with P_1 (respectively P_o), a P_1 -set (respectively a P_o -set), moreover if the corresponding k -set is a partition, we will name it a P_1 -partition (respectively a P_o -partition), eventually we will call a P_o -core, a P_o -set whose elements are β -core for a $\beta \in \mathbb{B}_n$.

We denote hereunder: $\mathcal{A} = (A_i)_{I_k}$ a P_1 -set of size k , with $k \geq 3$ (Hereunder $n \geq 3$). The question is :

$$\text{Does there exist such a set family of } G_n? \quad (6)$$

Such a set family if it exists, will be named a solution of size k for the problem P_1 .

Back to “Some elements to the general solution” XIV on page 29 Remarks:

- A P_o -set is a P_1 -set. A P_o -core which is a partition is a P_o -partition
Back to Property 1 footnote 54 on the following page
Back to equivalence P_1/P_o , proof in footnote 61 on page 23
Back to Theorem proof in footnote 67 on page 29
- $\varphi \in \mathcal{I}_{\text{som}}$, if $\mathcal{A}$ is a P_o -set (respectively a P_1 -set) then $\varphi\mathcal{A}$ is a P_o -set (respectively a P_1 -set).
Back to Property 2 footnote 57 on page 22 Back to case = 5 proof in footnote 2 on page 30
- If $\mathcal{A}$ is a P_o -set then $k \leq n$ and if $k = n$ then $\mathcal{A}$ is an equipartition.⁵⁰
Back to proof footnote 70 on page 31 Back to General case n footnote 66 on page 28
Back to Theorem proof: chapter XIV on page 29
Back to “Miscellaneous” XIII on page 28
And any element of $A \in \mathcal{A}$ belongs to a β -core whose cardinal is 2, for a $\beta \in \mathbb{B}_n$.⁵¹

⁴⁹

⁵⁰

Since each element of G_n , has n links (see: VIII on page 15), this means that any element of A_i having already a link in A_i , has only $n - 1$ links left to other A_j for $j \neq i$, henceforth $k - 1 \leq n - 1$ that is $k \leq n$.

If actually k does equal to n , since each element of A_i has only one link with an element of A_j , $j \neq i$; first there's no link left to reach out any element on $\mathbb{C}_{\cup A_i}^{I_n}$, so $\mathbb{C}_{\cup A_i}^{I_n} = \emptyset$ and $\mathcal{A}$ is a partition; second, A_i and A_j are in bijection since there is a link and only one link between two elements of them, so $\mathcal{A}$ is an equipartition (See figure: 3 on the following page).

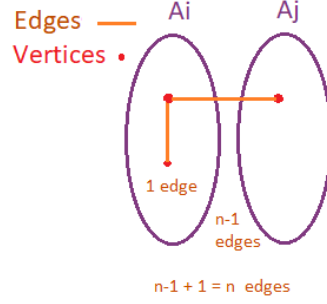
⁵¹

Since any element $a \in A \in \mathcal{A}$ has at least one internal link in A and at most one link in A to leave room for the links necessary towards the $n - 1$ other members of the partition $\mathcal{A}$.

- If $\mathcal{A}$ is a P_1 -set then $k \leq n+1$ and if $k = n+1$ then $\mathcal{A}$ is an equipartition.⁵²
And any $A \in \mathcal{A}$ is β -core free for any $\beta \in \mathbb{B}_n$.⁵³ [Back to unicity, proof in footnote 62 on page 24](#)
- $\forall A_i \in \mathcal{A}$, for $A_j \in \mathcal{A}$, $j \neq i$, $A_j \subset \mathbb{C}_{A_i}$ complies with P_1 . (see statement 4 on page 19)

[Back to Property 2 descaling footnote 55 on the next page](#)

Figure 3: The case P_o



Property 1:

If $\mathcal{A}$ is a solution of size n in G_{n-1} (i.e. a P_1 -partition of size n in G_{n-1}), then⁵⁴:

$$\left((1 + \beta_n)A_i\right)_{I_n} \text{ is a } P_o\text{-core of } \mathcal{P}(G_n) \quad (\text{thus a } P_o\text{-partition}) \quad (7)$$

[Back to case \$n = 4\$ footnote 63 on page 26](#) [Back to General case \$n\$ footnote 66 on page 28](#)

[Back to case \$n = 8\$ footnote 65 on page 27](#) [Back to proof equivalence solution \$P_1/P_o\$ footnote 61 on page 23](#)

52

The proof is similar to the one above in footnote 50 , except for now we must have $k-1 \leq n$

53

Since any $\gamma \in G_n$ can't have an internal link in any $A_i \in \mathcal{A}$

54

Proof:

Let $(B_i)_{I_k}$ be a P_1 -set of $\mathcal{P}(G_q)$, p, q defined in chapter VI "The subgroups of G_n ", ($k \leq |G_q|$).

- $G_p \times B_i \cap G_p \times B_j = G_p \times (B_i \cap B_j) = \emptyset$ for $i, j \in I_k$, $i \neq j$
- $\bigcup_{I_k} (G_p \times B_i) = G_p \times \bigcup_{I_k} (B_i) \subset G_p \times G_q \sim G_{p+q}$
- $G_p \times B_i \sim \pi_q(B_i)$ hence $G_p \times B_i$ satisfies P_1 , see equation 5 on the preceding page and notations in notations: VI on page 9
- $(1 + \beta_n)(G_p \times B_i) = (1 + \beta_p)G_p \times B_i = \emptyset$ (see in chapter VI on page 9), since $(1 + \beta_p)^2 = \emptyset$, hence $G_p \times B_i$ is a β_n -core and thus P_o holds (see in chapter XI on page 19).

So, $(G_p \times B_i)_{I_k}$ is a P_o -core of $\mathcal{P}(G_n)$

Applying this with $\mathcal{A} = (B_i)_{I_k}$, with $p = 1$, $q = n-1$, $k = n$, completes the proof. (see chapter XII on the preceding page)

Property 2:

- If we have a solution $(A_i)_{I_k}$ in G_n (i.e. a P_1 -partition of size k in G_n), k an integer strictly greater than 3, then for any $k' \in I_k$, we have a solution $(A_i)_{I_{k'}}$ in G_n ⁵⁵.
Back to existence theorem, consequences in footnote 67 on page 29
- If we have a solution $(A_i)_{I_{n+1}}$ in G_n (i.e. a P_1 -partition of size $n+1$ in G_n) then we have a solution of the form $(\beta A)_{\beta \in 1+\mathbb{B}_n}$, $A \in \mathcal{P}(G_n)$, with $1 \in A$ ⁵⁶. We will call it a standard solution for G_n .
Back to unicity, proof in footnote 62 on page 24
- If we have a P_o -partition of size n , then we have a P_o -partition of the form $(\beta A)_{\mathbb{B}_n}$, with $1, \beta_n \in A$, $A \in \mathcal{P}(G_n)$.⁵⁷ Back to equivalence P_1/P_o , proof in footnote 61 on the following page
Proof property 4, case P_o footnote 59 on the next page

Property 3:

- $(\beta A)_{\beta \in 1+\mathbb{B}_n}$, $A \in \mathcal{P}(G_n)$, a standard solution, $n \geq 3$ then:
 $\sigma_1^n \cap A = \emptyset$, $\sigma_2^n \cap A = \emptyset$, $|\sigma_3^n \cap A| = \frac{|\sigma_2^n|}{3}$.
Back to unicity, proof in footnote 62 on page 24
Back to case $n = 4$ footnote 63 on page 26
Consequence: For $n = 3$, $A = 1 + \sigma_3^3$, which is also the stabilizer of A ⁵⁸

55

Proof: $(A_i)_{I_{k'-1}}$, $\sum_{I_k \setminus I_{k'-1}} A_i$ does the job.

Obviously it's a k' -set which is a partition of G_n , and $\sum_{I_k \setminus I_{k'-1}} A_i \supset A'_k$ holds P_1 (see XII on the previous page)

56

Let's suppose that we have a solution $\mathcal{A} = (A_i)_{I_{n+1}}$, and let's choose the only $A \in \mathcal{A}$ which contains 1 ($1 \in A$).

Since A is β -core free for $\beta \in \mathbb{B}_n$, for $j \in I_n$ we have $\beta_j A \cap A = \emptyset$. Then if we have an element in $\beta_j A \cap \beta_k A$; $j \neq k$, $j, k \in I_n$ then there's a link from this element to two elements of A but this is impossible because an element of $G_n \setminus A$ can't have more than one link towards A : $\beta_j A \cap \beta_k A = \emptyset$. And so $(\beta A)_{1+\mathbb{B}_n}$ is a disjoint set family.

$\varphi_\beta A$ satisfies P_1 , for $\beta \in \mathbb{B}_n + 1$

$\sum_{1+\mathbb{B}_n} |\varphi_\beta A| = \sum_{1+\mathbb{B}_n} |A| = (n+1)|A| = |G_n|$. So $(\beta A)_{1+\mathbb{B}_n}$ is a solution.

Back to unicity, proof in footnote 62 on page 24

57

Let's suppose that we have $\mathcal{A}$, a P_o -partition, and let's choose an $A \in \mathcal{A}$, such that $1 \in A$, let a be an element in $\beta_i A \cap \beta_j A$, $i, j \in I_n$, $i \neq j$. So a has two links (β_i and β_j) towards A , whether a belongs to A or not this is impossible.

So $(\beta A)_{\mathbb{B}_n}$ is a disjoint family.

Now $|\sum_{\mathbb{B}_n} \varphi_\beta A| = \sum_{\mathbb{B}_n} |A| = n|A| = |G_n|$, hence $(\beta A)_{\mathbb{B}_n}$ is a P_o -partition (see in chapter XI on page 19).

we may assume that $\beta_n \in A$:

For an $i \in I_n$ well chosen $1 \in \beta_i A$, thus $\varphi_{(i,n)} A$ contains 1 and β_n and $(\beta \varphi_{(i,n)} A)_{\mathbb{B}_n}$ is a P_o -partition since $\varphi_{(i,n)}$ is an automorphism and an isometry (see VI on page 6, IX on page 15).

58

Let $\mathcal{A} = (A\beta)_{\beta \in 1+\mathbb{B}_n}$ be a solution of size $n+1$, $A \in \mathcal{P}(G_n)$, $1 \in A$.

$\beta_i, \beta_j \in 1+\mathbb{B}_n$, $\beta_i \neq \beta_j$, $\beta_i A \cap \beta_j A = \emptyset$

- for $i = 0$ since $1 \in A$ we get $A \cap \beta_j A = \emptyset \implies \beta_j \notin A$ so $A \cap \sigma_1^n = \emptyset$
- for $i \neq 0$ and $j \neq 0$ we get $\emptyset = \varphi_{\beta_j}(\beta_i A \cap \beta_j A) = \beta_i \beta_j A \cap A \implies \beta_i \beta_j \notin A$ so $A \cap \sigma_2^n = \emptyset$
- Each element of degree 3 in A generates exactly 3 elements of degree 2 in $\mathbb{C}_A$, necessarily different (and there are the whole lot of them since A has no element of degree 2). This means that $3|\sigma_3^n \cap A| = |\sigma_2^n|$
- If $n = 3$, since then $|A| = \frac{|G_3|}{4} = 2$ this clearly means that $A = 1 + \sigma_3^3$. Also the stabilizer of A which is included in A (see IX on page 18), is either A or 1, so it is A , because A is a group.

Property 4:

- If we have a standard solution $(\beta G)_{\beta \in 1+\mathbb{B}_n}$ (Or respectively a P_o -partition $(\beta G)_{\beta \in \mathbb{B}_n}$ in G_n , $1, \beta_n \in G$), $G \in \mathcal{P}(G_n)$, then: G is a subgroup of G_n ⁵⁹ [Back to unicity, proof in footnote 62 on the next page](#)

Consequence:

1. If we have a P_o -partition $(\beta G)_{\beta \in \mathbb{B}_n}$ in G_n , $1, \beta_n \in G$ subgroup of G_n , then G is β_n -core. ⁶⁰
2. We have a standard solution in G_{n-1} if and only if we have a P_o -partition in G_n ⁶¹

59

Let's assume that we have a standard solution in G_n , $\mathcal{A} = (\beta A)_{\beta \in 1+\mathbb{B}_n}$, $A \in \mathcal{P}(G_n)$.

Let G' be the stabilizer of A (see chapter IX on page 18), since $1 \in A$, $G' \subset A$ (see:IX on page 18).

Now, indeed there exists a standard solution: $\mathcal{G} = (\beta G)_{\beta \in 1+\mathbb{B}_n}$, G a subgroup of G_n (see footnote 66 on page 28).

Thus we have the commutative diagram of chapter: VI on page 10 with $\eta G'$ a subgroup of G . With:

$$G_n = \sum_{1+\mathbb{B}_n} \beta G = \sum_{1+\mathbb{B}_n} \beta A$$

Since $\pi_{\eta G'}(\beta G) \sim \beta G$ then : $\bigcup_{1+\mathbb{B}_n} \pi_{\eta G'}(\beta G) = \sum_{1+\mathbb{B}_n} \pi_{\eta G'}(\beta G)$, and similary since

$\pi_{G'}(\beta A) \sim \beta A$ then : $\bigcup_{1+\mathbb{B}_n} \pi_{G'}(\beta A) = \sum_{1+\mathbb{B}_n} \pi_{G'}(\beta A)$, so we have the following commutative diagram:

$$\begin{array}{ccc} \sum_{1+\mathbb{B}_n} \beta G & \xleftarrow{\eta} & \sum_{1+\mathbb{B}_n} \beta A \\ \pi_{\eta(G')} \downarrow & & \downarrow \pi_{G'} \\ \sum_{1+\mathbb{B}_n} \pi_{\eta(G')}(\beta G) & \xleftarrow{\tilde{\eta}} & \sum_{1+\mathbb{B}_n} \pi_{G'}(\beta A) \end{array}$$

In particular $\tilde{\eta}(1) = 1$ i.e. $G \sim \pi_{\eta(G')}(G) \xleftarrow{\tilde{\eta}} \pi_{\eta G'}(A) \sim A$, necessarily: $G = \eta(A)$, A is a group.

The proof for a P_o -partition is similar, note that the solution with the group $(1+\beta_n)G$ is $\mathcal{G} = (\beta(1+\beta_n)G)_{\beta \in 1+\mathbb{B}_{n-1}}$ see chapter 66 on page 28 and that for the solution $\mathcal{A} = (\beta A)_{\beta \in \mathbb{B}_n}$ accounted for, 1 and $\beta_n \in A$ (see chapter XII on the preceding page) and so with $A' = \beta_n A$, we consider $\mathcal{A} = (\beta A')_{\beta \in 1+\mathbb{B}_{n-1}}$

60

Let $\mathcal{A} = (\beta G)_{\mathbb{B}_n}$, $\beta_n \in G$ a subgroup of G_n , since $\beta_n \in G$ and G group, $\beta_n G = G$ which means that G is a β_n -core.

61

[Back to unicity, proof in footnote 62 on page 25](#)

- The condition is sufficient: If we have a solution $\mathcal{A} = (\beta G)_{1+\mathbb{B}_{n-1}}$ then $(1+\beta_n)\mathcal{A} = (\beta(1+\beta_n)G)_{1+\mathbb{B}_{n-1}} = (\beta(1+\beta_n)G)_{\mathbb{B}_n}$ is P_o -core (see XII on page 21), since $\beta_n(1+\beta_n) = 1+\beta_n$ and for $i, j \in \llbracket 0, n-1 \rrbracket$ $i \neq j$, $(1+\beta_n)(\beta_i G \cap \beta_j G) = \emptyset$ ($G \subset G_{n-1}$), and also $\beta_n \beta_i G \cap \beta_j G = \emptyset$ ($\beta_j G \subset G_{n-1}$ and $\beta_n \beta_i G \subset G_n \setminus G_{n-1}$) hence $(1+\beta_n)\beta_i G \cap (1+\beta_n)\beta_j G = \emptyset$ and $(1+\beta_n)\mathcal{A}$ is a P_o -partition in G_n (see XII on page 20).

- the condition is necessary: If we have a P_o -partition $\mathcal{A} = (\beta G)_{\mathbb{B}_n}$, with G a β_n -core (see in chapter: XII on the previous page), $\beta_n \in G$, then $G = (1+\beta_n)H$, H subgroup of G_n with $\beta_n \notin H$, see statement 3 on page 7
also $G = G \cap (G_{n-1} + \beta_n G_{n-1}) = G \cap G_{n-1} + \beta_n(G \cap G_{n-1})$, thus $H = G \cap G_{n-1} \subset G_{n-1}$ see statement VI on page 6,
 $\mathcal{A} = (\beta(1+\beta_n)H)_{\mathbb{B}_n}$ then $\pi_{n-1}(\mathcal{A})$ holds P_1 (see statement 5 on page 20) and since $\pi_{n-1}(\beta(1+\beta_n)H) \sim \beta H(1+\beta_n) = \beta G$ and that for $i, j \in \llbracket 0, n-1 \rrbracket$, $i \neq j$, $\beta_i G \cap \beta_j G = \emptyset$ then $\pi_{n-1}(\mathcal{A}) \in \mathcal{P}(G_{n-1})$ is a disjoint family, hence a standard solution.

- If there's a solution of size $n+1$ in G_n (Or equivalently a P_o -partition of size n in G_n) then it is unique up to bijective morphisms (a product of an isometry and an automorphism) of the form: $(\beta G)_{\beta \in 1 + \mathbb{B}_n}$ (Or respectively $(\beta G)_{\beta \in \mathbb{B}_n}$ that we will call a standard P_o -partition), G a subgroup of G_n .⁶²

Back to “Theorem”: chapter XIV on page 29

Back to “Epilog”: chapter XIX on page 38

⁶² Proof:

1. Let's have a solution: $\mathcal{A} = (A_i)_{[0, n]}$ up to a permutation in G_σ we may assume $1 \in A_o$. Since the only link to 1 is a $\beta \in \mathbb{B}_n$, necessarily, up to a permutation in G_σ , $\beta_i \in A_i$ for $i \in I_n$. And hence up to a permutation in G_σ , a solution is of the form: $(\beta_i A_i)_{[0, n]}$ where $A_i \ni 1$.
2. Let's have a solution $\mathcal{A} = (\beta_i A_i)_{[0, n]}$ where $A_i \ni 1$. From what precedes (see property 2 XII on page 22 and property 4 above, see XII on the preceding page), we know that A_o is a group of index $n+1$ in G_n and since $\varphi_{\beta_i} \mathcal{A}$ is also a solution, A_i is also a group of index $n+1$ in G_n for $i \in I_n$. So up to an isometry, a solution is always of the form $(\beta_i G_i)_{[0, n]}$ where G_i is a subgroup of index $n+1$ in G_n .
3. Let's revisit the property P_1 for a standard solution with the G group associated with:
 $\forall_G g \quad \forall_{I_n^2} (i, j), i \neq j \quad \exists_{I_n} k, k \notin \{i, j\}$ such that $\beta_k(\beta_i g) \in \beta_j G$ i.e. $\beta_i \beta_j \beta_k g \in G$
 Note that the k in question is unique (otherwise $k' \neq k, k' \in I_n, \beta_i \beta_j \beta_k \beta_{i'} \beta_j \beta_{k'} = \beta_k \beta_{k'} \in G$ impossible, see XII on page 22) and also doesn't depend on g ($\beta_i \beta_j \beta_k g \beta_{i'} \beta_j \beta_{k'} g' \in G, k, k' \in I_n, g, g' \in G$, then $\beta_k \beta_{k'} \in G, \beta_k \beta_{k'} = 1, k = k'$)

$$\text{and so we have the following scheme:} \quad \forall_{[0, n]^2} (i, j) \quad \exists! k \in [0, n] \quad \beta_i G \xrightarrow{\varphi_{\beta_k}} \beta_j G \quad (8)$$

Note also that since on one hand for the $\beta_i \beta_j \beta_k$ in question above it belongs to G (do $g = 1$ in the previous equation), and on the other hand $3|\sigma_3^n \cap G| = |\sigma_2^n|$ the whole lot of them are exactly $\sigma_3^n \cap G$.

Now $g \in G$ of degree greater than 3, we can construct a series in G : $g \xrightarrow{\gamma_1} g_1 \xrightarrow{\gamma_2} g_2 \dots \xrightarrow{\gamma_m} g_m \longrightarrow \dots, m \in \mathbb{N}^*$ by defining: $\gamma_m = \beta_i \beta_j \beta_k \in G$ whenever $\text{supp } g_{m-1}$ contains any pair $\{i, j\}$ (see Property in chapter III on page 3), $\gamma_m = 1$ otherwise. Hence, the series $(\deg(g_m))_{\mathbb{N}^*}$ is strictly decreasing until it ends up to zero. So for a $g \in G$ there exists an $m \in \mathbb{N}^*$ such that $g = \prod_{i=1, m} \gamma_i = 1, g = \prod_{i=1, m} \gamma_i$, henceforth $G = \langle \sigma_3^n \cap G \rangle$, G is generated by its elements of degree 3. In the following we will denote Γ (respectively Γ') a minimal (by cardinal) subset of $\sigma_3^n \cap G$ (respectively $\sigma_3^n \cap G'$) such that $G = \langle \Gamma \rangle$ (respectively $G' = \langle \Gamma' \rangle$), and $\tilde{\Gamma}$ a minimal (by cardinal) subset of $\sigma_3^n \cap (G \cap G')$ generating $G \cap G'$ and such that $\tilde{\Gamma} \subset \Gamma$ and $\tilde{\Gamma} \subset \Gamma'$ (It's always possible: necessarily $G \cap G'$ is generated by a subset $\tilde{\Gamma}$ of Γ and we can complete $\tilde{\Gamma}$ with elements of Γ' to obtain a new minimal set Γ' that generates G' , have a look at proof footnote 17 on page 7 as a hint).

4. Let's have a solution: $\mathcal{A} = (\beta_i G_i)_{[0, n]}$, G_i subgroup of G_n (necessarily of index $n+1$ in G_n , see property XII on page 21) let's consider the two solutions $(\beta_i G)_{[0, n]}$, with $G \stackrel{\text{def}}{=} G_o$ and $(\beta_i G')_{[0, n]}$, $G' \stackrel{\text{def}}{=} G_j$ for a $j \in I_n$, $G_n = \sum_{j \in [0, n]} \beta_j G = \sum_{j \in [0, n]} \beta_j G'$. G and G' are two isomorphic groups, $\psi G = G'$, ψ an isomorphism, $|G| = |G'|$.

For any (i, j) in $I_n^2, i \neq j$, there exist k, k' in $[0, n]$ such that we have the following scheme:

$$\begin{array}{ccc} & \varphi_{\beta_k} & \\ \beta_i G & \xrightarrow{\quad} & \beta_j G \\ & \varphi_{\beta_{k'}} & \\ \beta_i G' & \xrightarrow{\quad} & \beta_j G' \end{array}$$

Now there are two possible cases:

- Either, $\forall_{I_n^2} (i, j), i \neq j, \varphi_{\beta_k} = \varphi_{\beta_{k'}}$ which means that any $\gamma = \beta_i \beta_j \beta_k \in \Gamma$ also belongs to $G', G = \langle \Gamma \rangle \subset G', G = \langle \Gamma \rangle = G'$, hence $G_j = G$ for any $j \in I_n$.
- Or, $\exists_{I_n^2} (k, k'), k \neq k', \varphi_{\beta_k} \neq \varphi_{\beta_{k'}}$.
 Since there's only one link from an element of $\beta_i G \cap \beta_i G' \ni \beta_i$ towards $\beta_j G$ necessarily such an element is sent to $\beta_j G \setminus \beta_j (G \cap G')$ via φ_{β_k} and $\beta_j G' \setminus \beta_j (G \cap G')$ via $\varphi_{\beta_{k'}}$, and necessarily $G \neq G'$, technically:

$$\forall_{\beta_i (G \cap G')} g \quad \varphi_{\beta_k} g \in \beta_j G \setminus \beta_j (G \cap G') \quad (9)$$

(otherwise $\varphi_{\beta_k} g \in \beta_j (G \cap G') \subset \beta_j G', \varphi_{\beta_{k'}} g \in \beta_j G', \beta_k \beta_{k'} \in G', k = k'$ contrary to hypothesis). Which leads to:

$|\varphi_{\beta_k} \beta_i(G \cap G')| = |\beta_j G| - |\beta_j(G \cap G')|$, $2|G \cap G'| = |G|$, So the index of $H \stackrel{\text{def}}{=} G \cap G'$ in G or G' is two. Hence:

$$G = \langle \tilde{\Gamma} + \gamma \rangle = (1 + \gamma)H, \gamma \in \Gamma, \gamma \in G \setminus G \cap G', \quad G' = \langle \tilde{\Gamma} + \gamma' \rangle = (1 + \gamma')H, \gamma' \in \Gamma', \gamma' \in G' \setminus G \cap G',$$

$$G_n = \sum_{1+\mathbb{B}_n} \beta G = \sum_{1+\mathbb{B}_n} \beta(1 + \gamma)H, \quad G_n = \sum_{1+\mathbb{B}_n} \beta G' = \sum_{1+\mathbb{B}_n} \beta(1 + \gamma')H$$

From this we infer: $\gamma' \sum_{1+\mathbb{B}_n} \beta H = \gamma \sum_{1+\mathbb{B}_n} \beta H$, so $\exists_{\mathbb{B}_n} \beta \quad \exists_H h, \quad \gamma' \beta h = \gamma.1$ then $\gamma' H = \gamma \beta H$.

Finally in this second case there exists $\beta \in \mathbb{B}_n$ with: $G_n = \sum_{[0, n]} \beta_i(1 + \gamma)H = \sum_{[0, n]} \beta_i(1 + \beta\gamma)H$

From what precedes, denoting $\mathcal{B}$ the set family $(\beta_i H)_{[0, n]}$, $\mathcal{B}$ and $\varphi_{\beta}\mathcal{B}$ are disjoint set families and we have:

$$\sum_{[0, n]} \beta_i \gamma H = \sum_{[0, n]} \beta_i \beta \gamma H \quad \text{i.e.} \quad \sum_{[0, n]} \beta_i H = \sum_{[0, n]} \beta_i \beta H, \text{ necessarily:}$$

$\forall_{I_n} i \quad \exists_{I_n} j$, such that $\beta_i \beta \in \beta_j H$ i.e. $\beta_i \beta \beta_j \in H$.

Now let's get back to our original set family $\mathcal{A}$, we have thus:

$\beta_i G_i = (\beta_i + \beta_j \gamma_i) H_i$ where $\beta_j \in \mathbb{B}_n \setminus \beta_i$ ($j \neq i$) and $\gamma_i \in \Gamma$ with $H_i = \frac{G}{1 + \gamma_i}$,
for $j \in I_n$, it reads:

$\beta_j G_j = (\beta_j + \beta^j \gamma_j) H_j$ where $\beta^j \in \mathbb{B}_n \setminus \beta_j$ and $\gamma_j \in \Gamma$ with $H_j = \frac{G}{1 + \gamma_j}$.

Now $\beta_j H_j \cap \beta_j \gamma_i H_i = \beta_j (H_j \cap \gamma_i H_i)$. $\gamma_i \in \gamma_i H_i$ and $\gamma_i \in H_j = \frac{G}{1 + \gamma_j}$ this latter except for $i = j$, hence $i = j$,

$\beta_i G_i = \beta_i (1 + \gamma_i) H_i = \beta_i G$, φ_{β_i} bijection, $\boxed{G_i = G \text{ for any } i \in I_n}$

5. Now let's consider two standard solutions $\mathcal{A} = (\beta G)_{\beta \in 1 + \mathbb{B}_n}$ and $\mathcal{A}' = (\beta G')_{\beta \in 1 + \mathbb{B}_n}$, thus G and G' are two isomorphic groups via an automorphism η . $\eta \mathcal{A} = (\eta(\beta) G')_{\beta \in 1 + \mathbb{B}_n}$ is a disjoint set family so $\eta \mathcal{A}$ are the orbits of the action of G' onto G_n ($\beta, \beta' \in 1 + \mathbb{B}_n$, $\eta(\beta) G' \cap \beta' G' \neq \emptyset$, $\beta' \eta \beta \in G'$, $\eta(\beta) G' = \beta' G'$), $\eta \mathcal{A} = (\beta G')_{\beta \in 1 + \mathbb{B}_n}$, $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic.

This complete the proof, wrap up in a nutshell: a solution $\mathcal{A}$ of size $n + 1$ in G_n is isomorphic to a standard solution Std of the form $Std = (\beta G)_{\beta \in 1 + \mathbb{B}_n}$, G a subgroup of G_n that is: $\mathcal{A} = \varphi Std$ where φ is an element of $\mathcal{S}omAut(G_n)$.

Note: $\mathcal{S}omAut(G_n) = Aut(G_n) \mathcal{S}om$, since $G_{\sigma} \subset Aut(G_n)$, $G_{\gamma} Aut(G_n) = Aut(G_n) G_{\gamma}$ ($\eta \in Aut(G_n)$, $\gamma \in G_n$, $\eta \circ \varphi_{\gamma} = \varphi_{\eta \gamma} \circ \eta$).

Remark: $\varphi \in \mathcal{S}om$, $\varphi = \varphi_{\gamma} \circ \varphi_{\sigma}$, $\varphi_{\gamma} \in G_{\gamma}$, is $\mathcal{P}(G_n)$ -linear, and $\varphi_{\sigma} \in G_{\sigma}$, is an automorphism, see IX on page 15, now G subgroup of G_n : [Back to populate chessboard cells, in footnote 75 on page 34](#)

$$\varphi \left(\sum_{1+\mathbb{B}_n} \beta G \right) = \varphi_{\gamma} \circ \varphi_{\sigma} \left(\sum_{1+\mathbb{B}_n} \beta G \right) = \varphi_{\gamma} \left(\sum_{1+\mathbb{B}_n} \varphi_{\sigma} \beta \quad \varphi_{\sigma} G \right) = \varphi_{\gamma} \left(\sum_{1+\mathbb{B}_n} \beta \varphi_{\sigma} G \right) = \sum_{1+\mathbb{B}_n} \beta \varphi_{\gamma} (\varphi_{\sigma} G) = \sum_{1+\mathbb{B}_n} \beta \varphi G.$$

So we say that two standard solutions are isometric if their associated groups are.

For the case P_O : two P_O -partitions $(1 + \beta_{n+1}) \mathcal{A}$ and $(1 + \beta_{n+1}) \mathcal{A}'$ in G_{n+1} where $\mathcal{A}$ and $\mathcal{A}'$ with their respective group associated with, isomorphic (see footnote: 61 on page 23), are two isomorphic solutions (see above) that is there exists $\varphi \in \mathcal{S}omAut(G_n)$ such that: $\mathcal{A} = \varphi \mathcal{A}'$ thus $(1 + \beta_{n+1}) \mathcal{A} \sim G_1 \times \mathcal{A}' = 1 \times \varphi (G_1 \times \mathcal{A})$ and the two P_O -partitions are isomorphic, since $1 \times \varphi$ belongs to $\mathcal{S}om_1 Aut(G_1) \times \mathcal{S}om_n Aut(G_n) \subset \mathcal{S}om_{n+1} Aut(G_{n+1})$.

Example: For the case $n = 8$ hereunder, let G' be the group $(1 + \beta_3 \gamma) H$ with $H \stackrel{\text{def}}{=} \frac{G}{1 + \gamma}$ and $\gamma = \beta_1 \beta_2 \beta_4$, then $(G' \beta)_{\mathbb{B}_8}$ is a standard

solution, and the isomorphism ψ defined from G to G' by: $\begin{cases} \psi|_H &= 1|_H \\ \psi|_{\gamma H} &= \varphi_{\beta_3}|_{\gamma H} \end{cases}$ provides an automorphism of G_n , η

with $\eta G = G'$, and then $(G' \beta)_{\mathbb{B}_8} = \eta(G \beta)_{\mathbb{B}_8}$ (η is not an isometry though since $\deg(\gamma.1) = 3$ and $\deg(\eta \gamma. \eta 1) = \deg(\beta_3 \gamma) = 4$)

XIII The case P_o

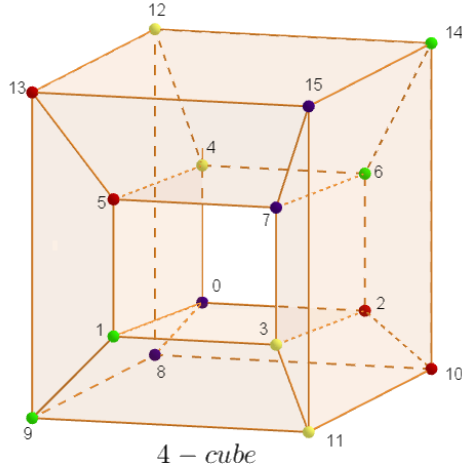
Back to “Solving the puzzle”: chapter XVI on page 31

Case $n = 4$

Hereunder in rows the 4-partition of G_4 complying with P_o in question⁶³. See figure 4:

$$\begin{aligned}
 1 + \beta_1\beta_2\beta_3 + \beta_4 + \beta_1\beta_2\beta_3\beta_4 &\sim \{0, 7, 8, 15\} && \text{see in chapter II on page 2} \\
 \beta_1 + \beta_2\beta_3 + \beta_1\beta_4 + \beta_2\beta_3\beta_4 &\sim \{1, 6, 9, 14\} \\
 \beta_2 + \beta_1\beta_3 + \beta_2\beta_4 + \beta_1\beta_3\beta_4 &\sim \{2, 5, 10, 13\} \\
 \beta_3 + \beta_1\beta_2 + \beta_3\beta_4 + \beta_1\beta_2\beta_4 &\sim \{4, 3, 12, 11\}
 \end{aligned}$$

Figure 4: A 4-cube P_o 4-partition



63

We look first for a 4-equipartition in G_3 which satisfies P_1 of the form $\mathcal{A} = (\beta G)_{\mathbb{B}_3+1}$, where $G = 1 + \sigma_3^3$ (see Property 3:XII on page 22).

Now let's consider orbit_G^3 with $G = 1 + \sigma_3^3$. Since G is a group (thus isomorphic to G_1 , see proposition 2 on page 7), and the stabilizer of G a subset of G (because $1 \in G$), the stabilizer of G , is G of index 4 in G_3 . G_3 is the direct product of G and G_2 (see VI on page 10), and $\text{orbit}_G^3 \sim G_3/G \sim G_2$ whose elements are classes of⁶⁴ $1, \beta_1, \beta_2, \beta_1\beta_2 \stackrel{\sigma_3^3}{\sim} \beta_3$, $\sum_{\text{orbit}_G^3} A = \sum_{\mathbb{B}_3+1} \beta G = \sum_{G_2} \beta G$, and $(A)_{\text{orbit}_G^3}$ is an equipartition of G_3 .

Note that for $\beta, \beta' \in \mathbb{B}_3 + 1$, necessarily $\beta\beta'G = \beta''G$ with $\beta'' \in \mathbb{B}_3 + 1$ since $\beta\beta'$ belongs to the orbits of G . Now let be $b \in G_3$, $b = \beta g$ with $\beta \in \mathbb{B}_3 + 1$ and $g \in G$: $d_3(b, \beta'G) = d_3(g, \beta''G) \leq d_3(g, \beta''g) = d_3(1, \beta'') \leq 1$, henceforth P_1 holds.

$(A)_{\text{orbit}_G^3}$ is a solution of size 4 in G_3 for P_1 .

From property 1 equation 7 on page 21 we know then that $((1 + \beta_4)(1 + \sigma_3^3)\beta)_{\mathbb{B}_3+1}$ is a P_o -core.
Nota: $(1 + \beta_4)(1 + \sigma_3^3) = 1 + \beta_1\beta_2\beta_3 + \beta_4 + \beta_1\beta_2\beta_3\beta_4$

64

$$\sum_{\mathbb{B}_3+1} \beta G \sim \sum_{\mathbb{B}_3+1} \pi_G(\beta) = \sum_{G_2} \pi_G \circ \eta(\beta) = \sum_{G_2} \bar{\eta} \circ \pi_2(\beta) = \bar{\eta} \left(\sum_{G_2} \pi_2(\beta) \right) \sim \sum_{G_2} \pi_2(\beta), \text{ see chapter VI on page 10}$$

Note that $(\pi_G(\beta))_{\mathbb{B}_3+1}$ holds P_1 , whereas $(\pi_2(\beta))_{G_2}$ doesn't ($\tilde{d}_2(\pi_2(\beta_1\beta_2), \pi_2(1)) = d_3(G_1 \times \beta_1\beta_2, G_1 \times 1) = 2 > 1$), in part because neither η nor $\bar{\eta}$ are isometries.

Case $n = 8$

Hereunder a 8-partition of G_8 complying with P_0 :

$$\boxed{\left((1 + \beta_8)\beta G\right)_{1+\mathbb{B}_7}} \quad 65$$

where G is the subgroup of G_7 of order $2^4 = 16$, generated by $\{\beta_1\beta_2\beta_4, \beta_2\beta_3\beta_5, \beta_1\beta_3\beta_6, \beta_1\beta_2\beta_3\beta_7\}$

65

We look first for a P_1 -partition of size 8 in G_7 , of the form $\sum_{1+\mathbb{B}_7} \beta G = \sum_{G_3} \beta G \sim \sum_{G_3} \beta G_4 \times 1_3$, where G is a subgroup of G_7 of order $\frac{|G_7|}{8} = |G_4|$, as such the sum would be actually a partition, as the classes of the elements of G_3 in G_7 for π_3 (see IX on page 18, with $q = 3$).

The subgroup of G_7 , $G = \langle \beta_1\beta_2\beta_4, \beta_2\beta_3\beta_5, \beta_1\beta_3\beta_6, \beta_1\beta_2\beta_3\beta_7 \rangle$ does the job, proof:

[Back to "General case, subgroup \$G\$ ": footnote 66 on the next page](#)

[Back to "Game strategy": chapter XVII on page 32](#)

Let's denote:

$$g_4 = \beta_1\beta_2\beta_4, \quad g_5 = \beta_2\beta_3\beta_5, \quad g_6 = \beta_1\beta_3\beta_6, \quad g_7 = \beta_1\beta_2\beta_3\beta_7$$

· About the first equality:

For $\beta_i \in 1 + \mathbb{B}_3$, $\beta_i \in G_3$

$$\beta_4 = \beta_1\beta_2g_4, \beta_5 = \beta_2\beta_3g_5, \beta_6 = \beta_1\beta_3g_6, \beta_7 = \beta_1\beta_2\beta_3g_7$$

· G is actually a subgroup of G_n of order 2^4 :

We have $\pi^4(\langle \beta_1\beta_2\beta_4, \beta_2\beta_3\beta_5, \beta_1\beta_3\beta_6, \beta_1\beta_2\beta_3\beta_7 \rangle) = \langle \beta_4, \beta_5, \beta_6, \beta_7 \rangle \xrightarrow{\varphi} G_4$ for a $\varphi \in G_\sigma$ well chosen, so $\pi^4(G) = \varphi G_4$, G is a subgroup of order greater than 2^4 , and it contains at most 2^4 elements, so it is isomorphic to G_4

· The partition satisfies P_1 :

This means that $\forall_{G_3} \beta, \beta', \forall_G g \quad (d_7(\beta g, \beta' G) \leq 1 \iff d_7(\beta \beta', G) \leq 1)$, which is equivalent to: $\forall_{G_3} \beta \quad \exists_G g \deg(\beta g) \leq 1$

For $\beta \in 1 + \mathbb{B}_3$ $\deg(\beta 1) \leq 1$

For $\beta \in G_3 \setminus \{1 + \mathbb{B}_3\}$, by construction $\exists_{[4, 7]} i \quad \beta \beta_i = g_i, \deg(\beta g_i) = \deg(\beta_i) = 1$, ok.

So $\mathcal{A} = (\beta G)_{G_3}$ is a solution of size 8 in G_7 .

Now we know from property 1 (see equation 7 on page 21) that

$(1 + \beta_8)\mathcal{A}$ is a P_0 -core of G_8 .

Find hereunder a complete description of G :

$$\begin{aligned} G = & \{g_4, & g_5, & g_6, & g_7 \\ & g_4g_5, & g_4g_6, & g_4g_7, \\ & g_5g_6, & g_5g_7, & g_6g_7, \\ & g_4g_5g_6g_7, & 1, \\ & g_5g_6g_7, & g_4g_6g_7, & g_4g_5g_7, & g_4g_5g_6\} \\ G = & \{\beta_1\beta_2\beta_4, & \beta_2\beta_3\beta_5, & \beta_1\beta_3\beta_6, & \beta_1\beta_2\beta_3\beta_7 \\ & \beta_1\beta_3\beta_4\beta_5, & \beta_2\beta_3\beta_4\beta_6, & \beta_3\beta_4\beta_7, \\ & \beta_1\beta_2\beta_5\beta_6, & \beta_1\beta_5\beta_7, & \beta_2\beta_6\beta_7, \\ & \sigma_7^7, & 1, \\ & \beta_3\beta_5\beta_6\beta_7, & \beta_1\beta_4\beta_6\beta_7, & \beta_2\beta_4\beta_5\beta_7, & \beta_4\beta_5\beta_6\} \end{aligned}$$

General case n , a power of two, a P_o -partition of G_n

[Back to Theorem: chapter XIV on the following page](#)

Hereunder a P_o -partition of G_n : [Back to Theorem proof in footnote 67 on the next page](#)

$$\boxed{((1 + \beta_n)\beta G)_{1+\mathbb{B}_{n-1}}} \quad 66$$

where G is a subgroup of G_{n-1} of index n , (see footnote 66 for a comprehensive description of this group) [Back to “Solving the puzzle”: chapter XVI on page 31](#)

[Back to Theorem proof: chapter XIV on the next page](#)

Miscellaneous

For $n = 3$ there is no P_o -partition since it should be an equipartition (see XII on page 20) but the cardinal of G_3 is prime to 3. And for the case $n = 2$, you’ll find a P_o -partition in the fig. : 2 on page 19, namely: $\{A, B\}, \{D, C\}$. The case $n = 1$ corresponding to the chessboard having only one tile is trivial, whereas the case $n = 0$, corresponds to the chessboard having no tile (So an empty partition would have been suitable but it’s not a P_o -set by definition).

66

[Back to “Epilog”: chapter XIX on page 37](#)

Since the P_o -partition in G_n if it exists, is an equipartition (see XII on page 20), 2 a prime and $|G_n| = 2^n$, n must be a power of 2, say: $n = 2^h$, $h \in \mathbb{N}$.

Let σ be an injection from $[1, n-1-h]$ to $G_h \setminus \{1 + \sigma_1^h\}$

Let’s define $\tilde{\psi}(i) = \beta_i \times \sigma_i$ for $i \in [1, n-1-h]$
def.

Now we have the injective group morphism:

$$I \subset I_{n-1-h}, \quad \begin{array}{ccc} G_{n-1-h} & \xrightarrow{\psi} & G_{n-1} \\ \prod_I \beta_i & \longmapsto & \prod_I \tilde{\psi}(i) \end{array}$$

Let’s denote η the embedding of G_{n-1} , $\psi \times 1_{G_h}$ (see :VI on page 10) and let’s posit: $G \stackrel{\text{def.}}{=} \eta(G_{n-1-h})$, then:

$$\sum_{G_h} \beta G = \sum_{1+\mathbb{B}_{n-1}} \beta G \quad \text{and} \quad \mathcal{A} \stackrel{\text{def.}}{=} (\beta G)_{1+\mathbb{B}_{n-1}} \text{ is a } P_1\text{-partition of } G_{n-1}$$

Proof: [Back to case “Theorem ”, consequences footnote 67 on the next page](#)

- ψ is a morphism: straightforward [Proof property 4, footnote 59 on page 23](#)
- ψ is injective: $I \subset I_{n-1-h}$, $1 = \psi(\prod_I \beta_i) = \prod_I \beta_i \times \sigma_i = \prod_I \beta_i \sigma_i = \prod_I \beta_i \prod_I \sigma_i$ the first term belongs to G_{n-1-h} the second one in G_h so in particular: $\prod_I \beta_i = 1_{G_{n-1-h}}$.
- the two expressions are equal:

For $\beta \in G_h$ such that $\beta \in 1 + \mathbb{B}_{n-1}$ there’s nothing to prove.

For $\beta \in G_h \setminus \{1 + \sigma_1^h\}$, there exists $i \in I_{n-1-h}$ such that $\sigma_i = \beta$, then $\eta(\beta_i \times 1_h) = \psi(\beta_i) = \beta_i \times \beta$ thus $\beta_i \times \beta \in G$, so:
 $\beta = (\beta_i \times 1_h)(\beta_i \times \beta)$, with $\beta_i \times 1_h \in \mathbb{B}_{n-1}$ and $\beta_i \times \beta \in G$

- Since G_n is the direct product of G and G_h (see VI on page 10), $\mathcal{A}$ is an equipartition.
- Since $\mathcal{A}$ is the orbit of G (G being the stabilizer), for any $\beta, \beta' \in 1 + \mathbb{B}_{n-1}$, there exists $\beta'' \in 1 + \mathbb{B}_{n-1}$ such that $\beta\beta'G = \beta''G$.
Now $\forall 1 + \mathbb{B}_{n-1} \beta, \beta' \quad \forall G g \quad d_{n-1}(\beta g, \beta' G) = d_{n-1}(g, \beta'' G) = d_{n-1}(\beta'', G) \leq d_{n-1}(\beta'', 1) \leq 1$, P_1 holds.

Nota: $G = \langle \sigma_i \beta_{i+h} \rangle_{[1, q]}$. Proof: $\pi^q(\langle \sigma_i \beta_{i+h} \rangle_{[1, q]}) = \langle \beta_{i+h} \rangle_{[1, q]} \sim G_q$ with $q = n-1-h$ and $G \supset \langle \sigma_i \beta_{i+h} \rangle_{[1, q]}$
[Back to “Solving the puzzle”: chapter XVI on page 31](#)

Now we know from property 1 (see equation 7 on page 21) that $((1 + \beta_n)\beta G)_{1+\mathbb{B}_{n-1}}$ is a P_o -core of G_n .

[Proof property 4, case \$P_o\$ footnote 59 on page 23](#)

XIV Existence and unicity theorem

In this chapter n is a non null integer.

Theorem

There exists a P_o -partition of size n in G_n if and only if n is a power of two

Back to “Solving the puzzle”: chapter XVI on page 31

Proof:

The condition is sufficient: since we can exhibit such a partition if n is a power of two (see in chapter XIII on the previous page).

The condition is necessary: since if we have a P_o -partition of size n in G_n , then it is an equipartition (see XII on page 20), so n divides $|G_n| = 2^n$.

Remark: According to chapter XII on page 24 when the solution exists it is unique up to bijective morphisms.

So now we know how to build up a P_o -partition of size n in the Eulerian n -cube graph or encode a number lower than $n - 1$ in a n -cube, when n is a power of two.

Consequences:

- h a non nul integer, for any $n \in \mathbb{N}$, $2^h - 1 \leq n < 2^{h+1} - 1$, we have a solution of any size lower or equal to 2^h in G_n ⁶⁷⁶⁷

Some elements on the general solution (6)

- Having a solution in G_n of the form $(A_i)_{I_n}$, $A_i \in \mathcal{P}(G_n)$, there's no solution in G_{n+1} of the form $(B_i)_{I_{n+1}}$, $B_i \in \mathcal{P}(G_{n+1})$ where $B_i \supset A_i$ for $i \in I_n$. Proof:⁶⁸⁶⁸
- Conversely if we have a solution in G_{n+1} of the form $(B_i)_{I_{n+1}}$, $B_i \in \mathcal{P}(G_{n+1})$ then we have no solution in G_n of the form $(A_i)_{I_n}$, $A_i \in \mathcal{P}(G_n)$, with $B_i \supset A_i$ for $i \in I_n$ (Otherwise it would contradict the previous statement).

67

Let's prove that under the conditions in question there exists a solution of size 2^h in G_n (see footnote XII on page 22).

According to theorem we have a P_1 -partition of size 2^h in G_{2^h-1} (see in chapter 66 on the preceding page): $(\beta_i G)_{[0, 2^h-1]}$ with G of index 2^h in G_{2^h-1} . Now: $(G_{n-2^h+1} \times \beta_i G)_{[0, 2^h-1]}$ is a solution of size 2^h in G_n .

Proof: $G_{n-2^h+1} \times G_{2^h-1} \sim G_n$ and for $s_1, s_2 \in G_{2^h-1}$,

$d_n(G_{n-2^h+1} \times s_1, G_{n-2^h+1} \times s_2) = d_{n-2^h+1}(G_{n-2^h+1}, G_{n-2^h+1}) + d_{2^h-1}(s_1, s_2)$ the first term being null (see VII on page 13).

68

Let's suppose that we have a solution $(A_i)_{I_n}$ in G_n , $A_i \in \mathcal{P}(G_n)$ and a solution $(B_i)_{I_{n+1}}$, $B_i \in \mathcal{P}(G_{n+1})$ where $B_i \supset A_i$ for $i \in I_n$. B_{n+1} must contain $\sum_{I_n} \beta_{n+1} A_i$ since for any element of A_i , $i \in I_n$ can't have another link to B_{n+1} than β_{n+1} (all the other links β_j , $j \in I_n$ sends an element of an A_i element to an element of $A_k \in \mathcal{P}(G_n)$). $\beta_{n+1} \sum_{I_n} A_i = \beta_{n+1} G_n$, since $G_{n+1} = \beta_{n+1} G_n + G_n$ (see VI on page 6), this means that $B_{n+1} = \beta_{n+1} G_n$ and $A_i = B_i$ for $i \in I_n$. But $\beta_{n+1} \sum_{I_n} A_i$ doesn't hold P_1 . Otherwise:

$\beta_{n+1} a_i \in \beta_{n+1} A_i$, $i \in I_n$ there exists $\beta \in \mathbb{B}_{n+1}$ such that $\beta \beta_{n+1} a_i \in A_j \subset G_n$, $j \in I_n$, we choose $i \neq j$. So $\beta \beta_{n+1} \in G_n$, thus $\beta \beta_{n+1} = 1$, $a_i \in A_j$, $A_i \cap A_j \neq \emptyset$ contrary to hypothesis, absurd.

· there's no solution of size 5 in G_5 ⁶⁹ (That is a P_1 -partition of size 5 in G_5).

XV The prisoners' conundrum

Back to “Game strategy”: chapter XVII on page 32

Back to “Let's play a bit with chessboard”: chapter XVII on page 34

A chessboard with a patchwork of white and black square tiles randomly laid out, possesses one tile under which the key to the prison cell is hidden.

The first prisoner who is shown where the key is, must flip the color of one tile (He turns a black tile into white, or a white one into black) and this is the only piece of information left to his cellmate who, with no more than a look at the chessboard has to devise where the hidden key tile is.

If he guesses correctly, both prisoners are set free. Back to “Abstract”: chapter I on page 1

This puzzle has been described here:

3 blue 1 brown puzzle: <https://www.3blue1brown.com/lessons/chessboard-puzzle>

XVI Solving the puzzle

We number the tiles of the chessboard with $\{1, 2, \dots, n\} = I_n$ ($n = 64$) and so a patchwork of black and white tiles is a n -tuple $(a_1, a_2, \dots, a_n) \in \mathbb{F}_2^n$ where:

$$\begin{aligned} a_i &= 0 && \text{if the } i\text{th tile is white} \\ &= 1 && \text{otherwise} \end{aligned}$$

69

Hereunder $n = 5$

If we have a solution of size n in G_n , then we have a solution of the form $(A_i)_{I_n}$, $A_i \in \mathcal{P}(G_n)$, with $1 \in A_1$ and $\beta_i \in A_i$ for $i = 2, \dots, n$.

Proof:

We may assume that $1 \in A_1$ (renumbering the indexes of the series $(A_i)_{I_n}$ should this be necessary), then the only link to 1 are the elements of $\mathbb{B}_n$, thus for A_1 to hold P_1 , for $i \in I_n \setminus \{1\}$, $\beta_i \in A_i$ (After possibly renumbering the series $(A_i)_{I_n}$, for $i = 2, \dots, n$).

So after renumbering there are two cases, case 1: $\beta_1 \in A_1$ and case 2: $\beta_1 \in A_2$.

Let's assume we have a solution of size n in G_n of the form $(A_i)_{I_n}$, $A_i \in \mathcal{P}(G_n)$, with $1 \in A_1$ and $\beta_i \in A_i$ for $i = 2, \dots, n$.

1. Whichever the case 1 or 2, for $i = 2, \dots, n$ A_i needs to contain at least $\frac{n-2}{2}$ elements of degree 2, to connect with at least $n-2$ elements of degree 1 in $G_n \setminus A_i$, n being odd this means that:

$$\text{for: } i = 2, \dots, n \quad |A_i \cap \sigma_2^n| \geq \frac{n-1}{2} \quad (10)$$

2. Note that once you have filled out A_i up to at least $\frac{n-1}{2}$ elements of degree 2, for $i = 2, \dots, n$, there are at most $\binom{n}{2} - (n-1)\frac{n-1}{2} = \frac{n-1}{2}$ elements left, to fill up the n subsets A_i with degree 2 elements and so for $i = 1, \dots, n$ necessarily there are at least $n - \frac{n-1}{2} = \frac{n+1}{2}$ indexes i for which $|A_i \cap \sigma_2^n| \leq \frac{n-1}{2}$

3. Since $(\varphi_{\sigma_2^n} A_i)_{I_n}$ is a solution (see XII on page 20), the rules 1. and 2. above apply to this solution. Now $|\varphi_{\sigma_2^n} A_i \cap \sigma_2^n| = |\varphi_{\sigma_2^n} (A_i \cap \varphi_{\sigma_2^n} \sigma_2^n)| = |A_i \cap \sigma_{n-2}^n|$ (see VI on page 7 and VI on page 8) and so the series $(|A_i \cap \sigma_{n-2}^n|)_{I_n}$ and $(|A_i \cap \sigma_2^n|)_{I_n}$ have the same pattern. In particular $(\sigma_{5-2}^5 = \sigma_3^5)$, the series $(|A_i \cap \sigma_2^5|)_{I_5}$ and $(|A_i \cap \sigma_3^5|)_{I_5}$ have the same pattern.

4. From what precedes, $n = 5$, to support P_1 , for at least $\frac{n+1}{2} = 3$ indexes $i \in I_n$, A_i must contain at least $\left(\binom{n}{2} - \frac{n-1}{2}\right) \frac{1}{\binom{3}{2}} = \frac{(n-1)^2}{6}$ elements of degree 3, actually 3 elements thanks to n odd, equal 5. But we know from 2.

and 3. there are at most $n - \frac{n+1}{2} = \frac{n-1}{2} = 2$ indexes $i \in I_5$ for which $|A_i \cap \sigma_3^5| > \frac{n-1}{2} = 2$, so it is impossible. The end of proof.

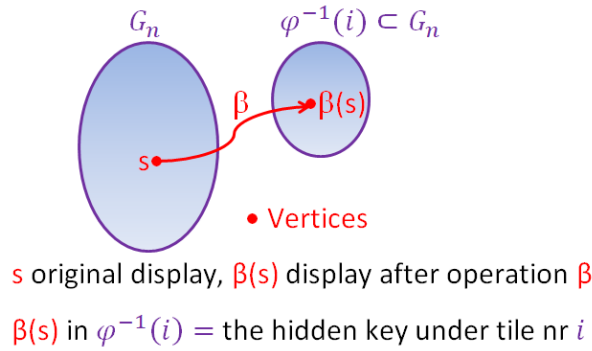
So basically, what the chessboard displays is a number in $\mathbb{F}_2^n \hookrightarrow \mathbb{N}$ (See chapter II on page 2). And what the first prisoner performs is an action $\beta \in \mathbb{B}_n$, on $\mathbb{F}_2^n \sim G_n$. (See chapter IV on page 3).

[Back to “Epilog”: chapter XIX on page 37](#)

If the second prisoner can infer the hidden key tile number from the number he reads on the chessboard this means that he possesses a mapping $\varphi \circ \varphi_\beta: G_n \longrightarrow I_n$, $\beta \in \mathbb{B}_n$, whose images are the hidden key tile numbers, and this is the only way to achieve this, technically we must have (see figure: 5):

$$P'_o: \quad \exists \varphi: G_n \supset D \longrightarrow I_n \quad \forall_{G_n} s \quad \forall_{I_n} i \quad \exists_{\mathbb{B}_n} \beta \quad \varphi \circ \varphi_\beta(s) = i$$

Figure 5: How to solve?



P'_o is equivalent to:

There exists a P_o -partition of G_n of size n (11)

[7070:Back to “Epilog”: chapter XIX on page 38](#)

The puzzle is solvable if and only if we have a P_o -partition of G_n of size n .

And according to theorem in Chapter XIV on page 29 such a partition actually does exist, if and only if n is a power of two, and 64 is:

70

Proof $P'_o \Rightarrow \exists P_o$ -partition :

Let's assume we have such a φ in P'_o . $D \subset G_n$ being the domain of φ , necessarily, $\varphi: D \longrightarrow I_n$ is surjective. $(\varphi^{-1}(i))_{I_n}$ is a n -set of G_n , and for a given $i \in I_n$ and $s \in G_n$ we can find a β in $\mathbb{B}_n$, such that: $\varphi \circ \varphi_\beta(s) = i$, thus $\varphi_\beta(s) = \beta s \in \varphi^{-1}(i)$, with $d_n(s, \beta s) = 1$, so $(\varphi^{-1}(i))_{I_n}$ is a P_o -set of size n , and from what precedes (see Remarks in chapter (XII on page 20)) we know it is a P_o -partition (hence $D = G_n$).

Proof $\exists P_o$ -partition $\Rightarrow P'_o$:

Let $(A_i)_{I_n}$ be a P_o -partition of G_n .

Let be $\varphi = \sum_{I_n} i \chi_i$ where χ_i :

$$\begin{aligned} \bigcup_{I_n} A_i & \xrightarrow{\chi_i} \{0, 1\} \\ x & \longmapsto \begin{cases} \chi_i(x) = 1 & \text{if } x \in A_i \\ \chi_i(x) = 0 & \text{otherwise} \end{cases} \end{aligned}$$

$\varphi: G_n \longrightarrow I_n$, is surjective. For any s in G_n , and i in I_n there exist $s_i \in A_i = \varphi^{-1}(i)$ and $\beta \in \mathbb{B}_n$ such that $\beta s = s_i$, since for A_i , P_o holds, $\varphi(\beta s) = i$, $\varphi \circ \varphi_\beta(s) = i$. So we posit $D \stackrel{\text{def}}{=} G_n$ and we are finished.

The puzzle is solvable

XVII Game strategy

Preliminaries

Back to “Epilog, calculus”: chapter XIX on page 38 Game rules here: chapter XV on page 30

Let G_h be the abelian group of order $2^h = n \in \mathbb{N}$ (see III on page 2). Bear in mind that we have the following property in G_h : $\forall G_h \beta \quad \beta^2 = \beta_0$ (β_0 the neutral element of G_h).

Let τ be a bijection which maps $I_n = \llbracket 1, n \rrbracket$ to G_h .

For $K \in \mathcal{P}(I_n)$ we define $\tau_K = \prod_K \tau(i) \in G_h$ ⁷¹

For a $\tau(key) \in G_h$ let k be the integer such that $\tau_K \tau(key) = \tau(k)$.⁷²

We posit $K^* = K + \{k\}$ Then: $\tau_{K^*} = \tau(key)$ ⁷³

.

71

$I_n \sim G_h$. Note that for:

$$H(\tau): \begin{matrix} \mathcal{P}(G_h) \sim G_n \\ K \end{matrix} \xrightarrow{H(\tau)} \begin{matrix} G_h \\ \tau_K = \prod_{\text{def. } K} \tau(i) \end{matrix} \quad \tau \text{ permutation of } G_h$$

$H(\tau)$ is a surjective homomorphism: $G_n \longrightarrow G_h$ Back to proof τ vs P_o -Partition in Epilog: footnote 76 on page 39

(We posit $\prod_{\emptyset} \tau(i) = \beta_0$)

Surjective: $\{\tau(i)\}_{I_n}$ contains n distinct elements $\rightsquigarrow = G_h$ | Homomorphism: $K, J \subset G_h, \tau_{K+J} = \prod_{K+J} \tau(i) = \prod_K \tau(i) \prod_J \tau(i) = \tau_K \tau_J$

And that: $H: \tau \longrightarrow H(\tau) \in \text{Hom}(G_n, G_h)$ is injective: τ, τ' permutations of G_h such that $H(\tau) = H(\tau')$

$\Rightarrow \forall \mathcal{P}(I_n) \quad K \quad \prod_K \tau(i) = \prod_K \tau'(i) \Rightarrow$ in particular $\forall G_h i \quad \tau(i) = \tau'(i)$ i.e. $\tau = \tau'$

72

Back to counting in Epilog: chapter 72

We say that two τ, τ' coding (i.e permutations of G_h) are equivalent if there's an automorphism $\sigma \in \text{Aut}(G_h)$ such that $\tau' = \sigma\tau$. Should this be the case, then we have: $\tau^{-1} \circ H(\tau) = \tau'^{-1} \circ H(\tau')$ Proof: $K \subset G_h, \tau' \circ \tau^{-1}(\tau_K) = \sigma(\tau_K) = \prod_K \sigma \circ \tau(i) = \prod_K \tau'(i) = \tau'_K$.

In particular for any $K \subset G_h, key \in G_h$:

$\tau^{-1}(\tau_{K+\{key\}}) = \tau'^{-1}(\tau'_{K+\{key\}})$; that is: $\tau^{-1}(\tau_K \tau(key)) = \tau'^{-1}(\tau'_K \tau'(key))$ (the τ and τ' deliver the same coding).

Conversely if $\tau^{-1} \circ H(\tau) = \tau'^{-1} \circ H(\tau')$ then $\tau' \circ \tau^{-1} \in \text{Aut}(G_h)$.

Proof:

$$\begin{aligned} \cdot \text{ for } K, J \subset G_h, \tau' \circ \tau^{-1}(H(\tau)(K)H(\tau)(J)) &= \tau' \circ \tau^{-1}(H(\tau)(K+J)) = H(\tau')(K+J) = H(\tau')(K)H(\tau')(J) = \\ &= \tau' \circ \tau^{-1}(H(\tau)(K))\tau' \circ \tau^{-1}(H(\tau)(J)) \\ &\tau' \circ \tau^{-1} \text{ is an endomorphism of } G_h \end{aligned}$$

$$\cdot (\tau' \circ \tau^{-1}) \circ \tau = \tau' \text{ is surjective, so is } \tau' \circ \tau^{-1}, \text{ henceforth } \tau' \circ \tau^{-1} \text{ is an automorphism.}$$

For $n = 64, h = 6$, there are $n! \simeq 10^{90}$ permutations of G_h . $\text{Aut}(G_h)$ acts on $\mathcal{T}(G_h)$ the permutations of G_h ($\sigma \in \text{Aut}(G_h), \tau \in \mathcal{T}(G_h), \sigma \cdot \tau = \sigma \circ \tau$). So with the methodology presented here, the number of non equivalent coding keys is the number of orbit in the above action: $\frac{n!}{|\text{Aut}(G_h)|} \simeq 10^{80}$, with $|\text{Aut}(G_h)| = \prod_{I_h} (2^h - 2^{k-1}) \simeq 10^{10}$ (see equality 1 on page 6), roughly the number of protons in the universe.

Back to “Epilog, calculus”: chapter XIX on page 38

73

Proof:

$$\tau_{K^*} = \prod_{K+\{k\}} \tau(i) = \prod_K \tau(i) \tau(k) = \tau_K \tau(k) = \tau(key)$$

Example: $n = 8, h = 3$

Notation: for $g = \prod_I \beta_i \in G_h$ where $I = \{i_0, i_1, i_2, \dots, i_{p-1}\}$ is an increasing injection from $\llbracket 0, p-1 \rrbracket$ to $\llbracket 1, h \rrbracket$ ($p \in \mathbb{N}^*, p-1 \leq h$), we denote g as $(i_{p-1} i_{p-2} \dots i_1 i_0)$, so $\prod_{\{1,3\}} \beta_i = \beta_3 \beta_1$ will be read (31) or 31

Below a description of a τ mapping (which essentially consists of populating randomly a n cell board with the elements of G_h), where we choose $\tau(key) = 321$, ($key \in I_n$):

0	1	2	3
21	31	32	$\tau(key)$

We say that the black tiles of the board stand for: $K = \{\tau^{-1}(1), \tau^{-1}(2), \tau^{-1}(31)\} \in \mathcal{P}(I_n)$.

We have:

- $\tau_K = (1)(2)(31) = 32 \in G_h$
- $\tau(k) = \tau_K \tau(key) = (32)(321) = 1^{74}74$
- We know from what precedes that: $\tau_{K^*} = \tau(key)$ with $K^* = K + \{\tau^{-1}(1)\} = \{\tau^{-1}(2), \tau^{-1}(31)\}$

And therefore the board K^* :

0	1	2	3
21	31	32	321

has a $\tau_{K^*} = (2)(31) = 321$ which is equal to $\tau(key)$ if we say that the black tiles stand for $K^* = \{\tau^{-1}(2), \tau^{-1}(31)\}$ and to generate it from the original board we only need to switch the color of the tile $k = \tau^{-1}(1)$ ($k \in I_n$) such that $\tau(k) = \tau_K \tau(key)$.

Given a τ mapping, in the following we will call K the black tiles or simply the board K , the corresponding value τ_K the **board value**, and $\tau(key)$ the **key tile**.

74

This is the reckoning of the actual operation in G_h group: $(\beta_2 \beta_3)(\beta_1 \beta_2 \beta_3) = \beta_1 \beta_2^2 \beta_3^2 = \beta_1$

XVIII Let's play a bit with the chessboard

Back to “Abstract”: chapter I on page 1 Game rules here: chapter XV on page 30

My cellmate and I agreed on this coding pattern ⁷⁵75, illustrated by the following chessboard:

0	1	2	21	3	31	32	321
4	41	42	421	43	431	432	4321
5	51	52	521	53	531	532	5321
54	541	542	5421	543	5431	5432	54321
6	61	62	621	63	631	632	6321
64	641	642	6421	643	6431	6432	64321
65	651	652	6521	653	6531	6532	65321
654	6541	6542	65421	6543	65431	65432	654321

Then the prison warden told me the key was hidden underneath the point of the “i” in the “Hi” and showed me this chessboard:

⁷⁵

$n = 64, h = 6, n^{\frac{1}{2}} = 8$

We considered the chessboard a matrix $(n^{\frac{1}{2}}, n^{\frac{1}{2}}) \in M_{n^{\frac{1}{2}}}(G_h)$ and for each cell (i, j) in $(I_{n^{\frac{1}{2}}})^2$ we first performed the following operations:

$$\left\{ \begin{array}{l} \text{For } (1, 1) \neq (i, j) \xrightarrow{\text{board numbering}} 8(i-1) + j - 1 \xrightarrow{\text{binary conversion}} \sum_{J_h} \delta_I(k) 2^k, I \subset J_h \xrightarrow{\mathbb{F}_2^h} (\delta_I(k))_{J_h} \xrightarrow{G_h} \prod_I \beta_{k+1} \\ \text{For } (1, 1) \xrightarrow{\text{board numbering}} n \xrightarrow{G_h} \beta_o = 1_{G_h} \end{array} \right.$$

where $J_h = \llbracket 0, h-1 \rrbracket$ and for $k \in J_h$ if $k \in I$ then $\delta_I(k) = 1$ and $\delta_I(k) = 0$ otherwise, see: III on page 3.

Then we put in cell (i, j) the value $\prod_I \beta_{k+1}$ or β_o whichever the case.

For instance:

Cell $(3, 7) \longrightarrow$ board square number: $22 \longrightarrow 2^4 + 2^2 + 2 \longrightarrow \sim (0, 1, 0, 1, 1, 0) \longrightarrow \sim \beta_5 \beta_3 \beta_2$ denoted (532) $I = \{1, 2, 4\}$
In the 22sd square of the grid we put the tag 532. And the top left board square is numbered n and filled out with (0) .

Remark: Any permutation of the elements in the cells of this grid would work, as well as any finite series of such kind of operations on the chessboard would end up with an operational coding (Because those are isometries. See footnote 62 on page 25).

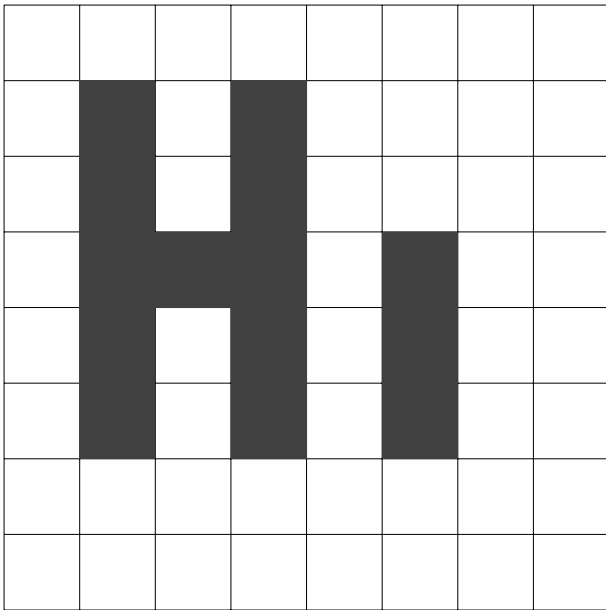
Which I swiftly encoded like this:

0	1	2	21	3	31	32	321
4	41	42	421	43	431	432	4321
5	51	52	521	53	531	532	5321
54	541	542	5421	543	5431	5432	54321
6	61	62	621	63	631	632	6321
64	641	642	6421	643	6431	6432	64321
65	651	652	6521	653	6531	6532	65321
654	6541	6542	65421	6543	65431	65432	654321

1. The **key tile** is: 431
2. With the black tiles: $\{41, 421, 431, 51, 521, 541, 542, 5421, 5431, 61, 621, 631, 641, 6421, 6431\}$
I calculated the **board value** which is the product:
 $(41)(421)(51)(521)(431)(541)(542)(5421)(5431)(61)(621)(631)(641)(6421)(6431) = 0$
See hereunder 1 on the next page an example how to handle this kind of multiplication (A lot simpler than the one you learn at primary school).
3. $(\text{board value})(\text{key tile}) = (0)(431) = 431$

Hence I flipped the color of the 431 tile.

And my cellmate has been shown this chessboard:



I was a bit afraid his messing up with the decoding but he did great, and we were set free after all.

How did he do it?

He filled out the chessboard like this:

0	1	2	21	3	31	32	321
4	41	42	421	43	431	432	4321
5	51	52	521	53	531	532	5321
54	541	542	5421	543	5431	5432	54321
6	61	62	621	63	631	632	6321
64	641	642	6421	643	6431	6432	64321
65	651	652	6521	653	6531	6532	65321
654	6541	6542	65421	6543	65431	65432	654321

1. Then he retrieved the black tiles:

$\{41, 421, 51, 521, 541, 542, 5421, 5431, 61, 621, 631, 641, 6421, 6431\}$ according to board.

Whose product of elements : $(41)(421)(51)(521)(541)(542)(5421)(5431)(61)(621)(631)(641)(6421)(6431)$

yields the **board value**. Details for this calculation: [Back to “encoding”: chapter 2 on the preceding page](#) In this product there are:

- 13 figures 1 $\rightsquigarrow$ 13, odd $\rightsquigarrow$ figure 1 appears in the calculated product
- 6 figures 2 $\rightsquigarrow$ 6, even $\rightsquigarrow$ zero appearance of 2 in the calculated product
- 3 figures 3 $\rightsquigarrow$ 3, odd $\rightsquigarrow$ figure 3 appears in the calculated product
- 9 figures 4 $\rightsquigarrow$ 9, odd $\rightsquigarrow$ figure 4 appears in the calculated product
- 6 figures 5 $\rightsquigarrow$ 6, even $\rightsquigarrow$ zero appearance of 5 in the calculated product
- 6 figures 6 $\rightsquigarrow$ 6, even $\rightsquigarrow$ zero appearance of 6 in the calculated product

Thus the **board value** is 431 (In the final product result appear only digits whose count is odd)

2. At this stage the **board value** gives the **key tile**, so the key is hidden under the tile tagged 431.

I wondered whether on a hunch he might have pinpointed to the missing point of the “i”, though it’s very unlikely, what do you think ? (I didn’t dare to ask).

XIX Epilog

Let’s get back to our n -cube $\sim G_n = \langle \beta_i \rangle_{I_n}$ (see chapter V on page 4, chapters III on page 2 and VI on page 6) where i is the chessboard tile number (see XVI on page 30), from tools described above, we have two isomorphisms $\theta = 1_{\langle \beta_n \rangle} \times \eta^{-1}$ (see footnote 66 on page 28 and chapter VI on page 10 with $n-1$ instead of n), along with a subgroup $L = (1 + \beta_n)G$ of index n in G_n which passes to the quotient with the following commutative diagram, and μ^* (see III on page 3):

$$\begin{array}{ccc} G_n & \xleftarrow{\theta} & G_n \xleftarrow{\mu^*} \mathcal{P}(I_n) \\ \pi_h \downarrow & & \downarrow \pi_L \\ G_h \sim \sum_{G_h} \beta G_{n-h} & \xleftarrow{\bar{\theta}} & \sum_{I_n} \beta_i L \end{array}$$

Back to defining “*hom*”, Epilog proof in footnote 76 on page 40

Basically flipping of a tile is a multiplication by a β_j in G_n of a board consisting of its black tiles

$K \in \mathcal{P}(I_n) \xrightarrow{\mu^*} \prod_K \beta_i \in G_n$ (see chapters III on page 3, XVI on page 31 and IV on page 4), which conveys a multiplication in G_h through $\bar{\theta} \circ \pi_L(\beta_j)$ for $j \in \llbracket 1, n \rrbracket = I_n$.

Notice that for any $i \in I_n$, $\bar{\theta}(\beta_i L) = \beta G_{n-h}$, for a unique $\beta \in G_h$ ($\bar{\theta}$ is an isomorphism see chapter VI on page 10 and footnote 66 on page 28). So basically $\tilde{H} = \bar{\theta} \circ \pi_L \circ \mu^*$ is a surjective homomorphism in $\text{Hom}(\mathcal{P}(I_n), G_h)$ which supports such a multiplication, and whose restriction to the singletons of $\mathcal{P}(I_n)$ is a bijection τ which maps I_n to G_h .

Now exploiting the properties of the G_n groups, having a $key \in I_n$, for any board $K \in \mathcal{P}(I_n)$ observe that we have a unique $k \in I_n$ such that:

$$\tau(k) = \tilde{H}(key + K), \quad \tilde{H}(key + K) = \tilde{H}(key) \tilde{H}(K) = \tau(key) \tilde{H}(K) \quad (12)$$

which leads to:

$$\tilde{H}(k + K) = \tau(k) \tilde{H}(K) = \tau(key) \tilde{H}(K)^2 = \tau(key) \quad (13)$$

Back to “Populating the chessboard grid”: footnote 75 on page 34

And so the board $k + K$ which essentially is the board K where tile k has been flipped, directly yields the value of the key tile thanks to $\tilde{H}$ decoding key. Note that since we only manipulate the values of $\tilde{H}(\{i\})$ for tile i , since $\tilde{H}(\sum_K i) = \prod_K \tilde{H}(i)$ ($\tilde{H}$ is a homomorphism) you only need to know the values of $\tilde{H}$ on the singletons of $\mathcal{P}(I_n)$, actually the image of τ , i.e the value in G_h you assign to a tile, basically: how you populate your

chessboard cells with the values of G_h .

Now it is clear that with this method any homomorphism in $\text{Hom}(\mathcal{P}(I_n), G_h)$ whose restriction to the singletons of $\mathcal{P}(I_n)$ is a bijective mapping to G_h would do the job (see in Preliminaries such a homomorphism in chapter XVII on page 32).

Also since finding a solution to the puzzle revolves around finding a subgroup of the n -cube, and that this subgroup is unique up to bijective morphisms (see chapter XII on page 24 and statement 11 on page 31), the method presented here is the unique way up to bijective morphisms to solve the puzzle.

The calculus shows that with that method there are as many non-equivalent ways of choosing the $\tilde{H}$ coding key as the number of protons in the universe (see bottom of footnote 72 on page 32 and footnote 7676 on the next page below), therefore would you make use of a quantum computer you won't crack this code any soon.

The end



Finding a P_O -partition in the n -cube or choosing a coding with τ in $\mathcal{T}(G_h)$ is the same, hereunder the proof.

Let be v a bijection, $v:$

$$G_h \xrightarrow{v} I_n$$

This provides us with an isomorphism, $v^*:$

$$\begin{array}{ccc} \mathcal{P}(G_h) & \xrightarrow{v^*} & \mathcal{P}(I_n) \\ K = \sum_K \gamma & \longmapsto & \sum_K v(\gamma) = v^*(K) \end{array}$$

Let $\text{Hom}(G_n, G_h)^*$ be the set of homomorphisms $\varphi \in \text{Hom}(G_n, G_h)$ such that $\varphi(\mathbb{B}_n) = G_h$.
Bear in mind that for $\varphi \in \text{Hom}(G_n, G_h)$, we have $\tilde{\varphi}$ a unique isomorphism with this commutative diagram:

$$\begin{array}{ccc} G_n & \xrightarrow{\varphi} & G_h \\ \pi \downarrow & \nearrow \tilde{\varphi} & \\ G_n / \text{Ker} \varphi & & \end{array} \quad \pi \text{ the canonical projection.}$$

And for example, $\varphi(\mathbb{B}_n) = G_h \iff \tilde{\varphi} \circ \pi(\mathbb{B}_n) = G_h \iff \pi(\mathbb{B}_n) \sim G_h$

Let's consider: $H: \mathcal{T}(G_h) \longrightarrow \text{Hom}(G_n, G_h)^*$ where:

$$H(\tau): \begin{array}{ccc} G_n & \xrightarrow{H(\tau)} & G_h \\ g & \longmapsto & \prod_{v^{*-1} \circ \mu^{*-1}(g)} \tau(i) \end{array} \quad \tau \text{ permutation of } G_h$$

· τ permutation of G_h , $H(\tau) \in \text{Hom}(G_n, G_h)^*$:

$$H(\tau)(\mathbb{B}_n) = \sum_{v^{*-1}(I_n)} \tau(i) = G_h.$$

· We already know that: H is injective (see 71 on page 32).

· Let's prove that H is surjective:

For l in $\text{Hom}(G_n, G_h)^*$, $g \in G_n$

$$l \circ \mu^* \circ v^*|_{G_h} \in \mathcal{T}(G_h), \text{ indeed: } l \circ \mu^* \circ v^*(G_h) = l(\mathbb{B}_n) = G_h.$$

$$H(l \circ \mu^* \circ v^*|_{G_h})(g) = \prod_{v^{*-1} \circ \mu^{*-1}(g)} l \circ \mu^* \circ v^*(i) = l\left(\prod_{v^{*-1} \circ \mu^{*-1}(g)} \mu^* \circ v^*(i)\right) = l(g).$$

· So H is a bijection.

Now, since, for $\sigma \in \text{Aut}(G_h)$ and $\tau \in \mathcal{T}(G_h)$, $H(\sigma \cdot \tau) = \sigma \cdot H(\tau)$, a coding actually is an element of $H(\mathcal{T}(G_h)) / \text{Aut}(G_h)$, see 71 on page 32. We call $\pi_{\text{Aut}(G_h)}$ the canonical projection from $\text{Hom}(G_n, G_h)^*$ onto $\text{Hom}(G_n, G_h)^* / \text{Aut}(G_h)$.

Let be $P_L = \left\{ L, \text{ subgroup of } G_n \text{ such that } (\beta L)_{\mathbb{B}_n} \text{ is a } P_O\text{-partition} \right\}$, now consider the map:

$$\begin{aligned} \text{hom: } \begin{matrix} P_L & \xrightarrow{\text{hom}} & H(\mathcal{T}(G_h))/\text{Aut}(G_h) \\ L' & \longmapsto & \Pi_{\text{Aut}(G_h)}(\pi_h \circ \theta \circ \Omega^{-1}) \end{matrix} \end{aligned}$$

where $\Omega \in \text{Aut}(G_h)$ an embedding of ω , an isomorphism such that $\omega(L) = L'$, (See property VI on page 10 and statement 2 on page 7)
and $\pi_h \circ \theta = \bar{\theta} \circ \pi_L$, θ defined in chapter Epilog above

Ω passes to the quotient as $\bar{\omega}$ (see: VI on page 11), and we have the following commutative diagram:

$$\begin{array}{ccccc} G_n & \xleftarrow{\theta} & \sum_{\mathbb{B}_n} \beta L & \xrightarrow{\Omega} & \sum_{\mathbb{B}_n} \beta L' \\ \pi_h \downarrow & & \pi_L \downarrow & & \pi_{L'} \downarrow \\ G_h & \xleftarrow{\bar{\theta}} & G_n / L & \xrightarrow{\bar{\omega}} & G_n / L' \sim G_h \end{array} \quad \pi_h \circ \theta \circ \Omega^{-1}(\mathbb{B}_n L') = \pi_h \circ \theta(\mathbb{B}_n L) = \pi_h(G_n) \sim G_h$$

• *hom* is well defined:

- It doesn't depend on the choice of ω . Let be ω' such that $\omega'(L) = L'$ and Ω' an associated embedding whose passage to quotient is $\bar{\omega}'$.
We have: $\pi_h \circ \theta \circ \Omega^{-1} = \bar{\theta} \circ \bar{\omega}^{-1} \circ \pi_{L'}$, and since $\text{Aut}(G_h)$ is a group there exists *aut* in $\text{Aut}(G_h)$ such that $\text{auto} \circ \bar{\theta} \circ \bar{\omega}^{-1} = \bar{\theta} \circ \bar{\omega}'^{-1}$, hence: $\text{auto} \circ \bar{\theta} \circ \bar{\omega}^{-1} \circ \pi_{L'} = \bar{\theta} \circ \bar{\omega}'^{-1} \circ \pi_{L'}$
- From above in particular: $\bar{\theta} \circ \pi_L \circ \Omega^{-1}(\mathbb{B}_n) = \bar{\theta} \circ \pi_{L'} \circ \Omega'^{-1}(\mathbb{B}_n L') \sim G_h$

• *hom* is injective:

We have: $\mathcal{Ker}(\pi_h \circ \theta \circ \Omega^{-1}) = \mathcal{Ker}(\bar{\theta} \circ \pi_{L'} \circ \Omega'^{-1}) = L'$

Let be $L', L'' \in P_L$, such that: $\text{hom}(L') = \text{hom}(L'')$, $\bar{\theta} \circ \pi_{L'} \circ \Omega'^{-1} = \text{auto} \circ \bar{\theta} \circ \pi_{L''} \circ \Omega''^{-1}$ with *aut* $\in \text{Aut}(G_h)$ and $\omega'(L) = L'', \Omega'$ an embedding of ω' , in particular $\mathcal{Ker}(\bar{\theta} \circ \pi_{L'} \circ \Omega'^{-1}) = \mathcal{Ker}(\bar{\theta} \circ \pi_{L''} \circ \Omega''^{-1})$, i.e $L' = L''$.

• Let's prove that *hom* is surjective.

$\varphi \in \text{Hom}(G_n, G_h)^*$: $\varphi\left(\sum_{\mathbb{B}_n} \beta\right) = G_h$, φ is a bijection from $\mathbb{B}_n$ to G_h , $\varphi\left(\sum_{\mathbb{B}_n} \beta \mathcal{Ker} \varphi\right) = G_h$

and thus $\bigcup_{\mathbb{B}_n} \pi(\beta) = \sum_{\mathbb{B}_n} \pi(\beta)$, and necessarily $\sum_{\mathbb{B}_n} \beta \mathcal{Ker} \varphi = G_n$, so because of the cardinals of the sets in question, we have the following commutative diagram:

$$\begin{array}{ccc} G_n & \xleftarrow{\quad} & \sum_{\mathbb{B}_n} \beta \mathcal{Ker} \varphi \\ \pi_h \downarrow & \nearrow \varphi & \downarrow \pi \\ G_h & \xleftarrow{\tilde{\varphi}} & \sum_{\mathbb{B}_n} \pi(\beta) \end{array}$$

Note that $(\beta \mathcal{K}er\varphi)_{\mathbb{B}_n} \sim (\pi(\beta))_{\mathbb{B}_n}$ is a P_O -partition (because these are the orbits of the action of $\mathcal{K}er\varphi$ onto G_n).

So $\boxed{\mathcal{K}er\varphi \in P_L}$.

Let ω be an isomorphism such that: $\mathcal{K}er\varphi = L' = \omega(L)$. In such a case $\pi = \pi_{L'}$.

Since $\text{Aut}(G_h)$ is a group there exists $\tilde{k} \in \text{Aut}(G_h)$ such that $\tilde{k}\tilde{\omega}\tilde{\omega} = \tilde{\theta}$, with the following commutative diagram:

$$\begin{array}{ccccc}
 G_n & \xleftarrow{\theta} & G_n & \xrightarrow{\Omega} & G_n \\
 \pi_h \downarrow & & \pi_L \downarrow & & \downarrow \pi \\
 G_h & \xleftarrow{\tilde{\theta}} & G_n/L \sim G_h & \xrightarrow{\tilde{\omega}} & G_n/L' \\
 & \nwarrow \tilde{k}\tilde{\omega} & & \nearrow &
 \end{array}$$

- $\pi_h \circ \theta \circ \Omega^{-1} = \tilde{k} \circ \tilde{\omega} \circ \pi = \tilde{k} \circ \varphi$, i.e $\text{hom}(\mathcal{K}er\varphi) = \pi_{\text{Aut}(G_h)}(\varphi)$
- Hence hom is a bijection.

$P_L \stackrel{\text{hom}}{\sim} H(\mathcal{T}(G_h))/\text{Aut}(G_h)$, the end of proof.